Mykhailo Fedorov, nhân vật chủ chốt trong chiến tranh drone của Ukraine

Từ nhà nước trong điện thoại thông minh đến Bộ Quốc phòng của cuộc chiến drone

Luật sư Kim Kyung-jin

AI Library - kimkj.com - 2026

Mục lục

Lời nói đầu. Từ một quốc gia trong chiếc điện thoại thông minh đến chiến trường

Lời hứa đưa chính phủ lên màn hình điện thoại thông minh, trong thời bình, nghe giống như ngôn ngữ của sự tiện lợi. Đó là lời hứa rằng việc lấy giấy tờ, nộp thuế và chứng minh danh tính chỉ cần vài cử động của ngón tay. Khi lực lượng Nga vượt qua biên giới vào tháng 2 năm 2022, màn hình ấy nhận thêm công việc khác. Nó trở thành quầy tiếp nhận nơi tiền được gửi cho người tị nạn, nơi nhà cửa bị phá hủy được báo cáo, nơi vị trí quân địch được thu thập, và nơi liên lạc ở tiền tuyến được giữ cho không đứt đoạn.

Người thúc đẩy sự thay đổi ấy là Mykhailo Fedorov. Ông phụ trách mảng kỹ thuật số trong chiến dịch tranh cử của Zelensky, rồi trở thành bộ trưởng ở tuổi hai mươi tám. Diia, IT Army, Starlink, UNITED24, Brave1, một đội quân drone — những cái tên này lần lượt gắn vào hồ sơ của ông. Tháng 1 năm 2026, ông trở thành bộ trưởng quốc phòng. Người từng thiết kế một quốc gia bên trong điện thoại thông minh được giao vũ khí và nhân lực, mua sắm công và dữ liệu, của một đất nước đang có chiến tranh.

Không có câu chuyện anh hùng nào được dựng lên ở đây. Thông cáo của chính phủ được để trong lời của chính phủ, thông cáo doanh nghiệp trong lời của các công ty, chỉ trích từ các chương trình phát trên YouTube được giữ như tuyên bố của người đã nói ra. Nơi nào một con số không có mẫu số, khoảng trống ấy được để lộ. Lý do tuổi thơ và lịch sử gia đình của ông không được viết dài cũng như vậy. Ngay khoảnh khắc một khoảng trống được lấp bằng một câu nghe có vẻ hợp lý, tiểu sử biến thành tiểu thuyết.

Sự nghiệp của Fedorov cho thấy công nghệ và quyền lực có thể kéo lại gần nhau nhanh đến mức nào. Đội ngũ xây dựng một ứng dụng đã đi đến chỗ xử lý dữ liệu chiến trường, và người từng nuôi dưỡng các startup lên nắm bộ phụ trách ký hợp đồng với chính những công ty ấy. Trong một cuộc chiến nơi tốc độ cứu mạng người, thủ tục chậm chạp rất khó chịu đựng. Nhưng khi thủ tục đã bị gỡ bỏ, câu hỏi ai đã quyết định và ai chịu trách nhiệm vẫn còn đó.

Mốc tham chiếu là ngày 13 tháng 7 năm 2026. Cuộc chiến chưa kết thúc, và nhiệm kỳ của Fedorov cũng chưa khép lại. Đây không phải là câu chuyện về một cuộc đời đã hoàn tất, mà là bản ghi giữa chừng về một quyền lực vẫn đang chuyển động. Ngay cả ở chương cuối, việc phán xét cũng không bị thúc ép. Những gì đã sáng tỏ được viết thật chính xác, còn những tuyên bố chưa được kiểm chứng thì được đánh dấu rõ ở phần rìa của chúng. Trước khi độc giả thích hay ghét Fedorov, tôi mong họ có thể nhìn thấy trước tiên cách hệ mạch mà ông xây dựng đã thực sự vận hành ra sao.

Tháng 7 năm 2026, Attorney Kim Kyung-jin

Chương 1. Một bộ trưởng 28 tuổi và cuộc cách mạng Diia

Ngày 29 tháng 8 năm 2019, quốc hội Ukraine phê chuẩn danh sách thành viên của nội các mới. Bộ Chuyển đổi Số lần đầu tiên ra đời vào ngày hôm đó, và Mykhailo Fedorov, hai mươi tám tuổi, trở thành bộ trưởng đầu tiên của bộ này. Mục tiêu mà ông công bố là "nhà nước trong điện thoại thông minh."

Trong hồ sơ công khai, việc ông sinh năm 1991 và mọi việc ông làm trước năm 2019 đều dựa trên một tài liệu bậc ba duy nhất. Phép tính cho thấy ông hai mươi tám tuổi vào thời điểm được bổ nhiệm là đúng. Nhưng chưa có tài liệu gốc nào được tìm thấy để chứng minh cụm từ thường đi sau tên ông, "bộ trưởng trẻ nhất trong lịch sử Ukraine." Vì vậy, thay vì dựng lại tuổi trẻ của ông, chúng ta bắt đầu từ những gì còn lại: một ứng dụng, một hệ thống luật, một nền tảng trao đổi dữ liệu, các báo cáo của những tổ chức quốc tế, và những chỉ trích gắn với tất cả những thứ đó. Lấp đầy một vai trò không có hồ sơ bằng câu chuyện chỉ làm câu văn dài hơn mà không thêm nền tảng nào bên dưới.

1. Chiến lược gia kỹ thuật số của một chiến dịch tranh cử bước vào chính phủ

Trong cuộc bầu cử tổng thống Ukraine năm 2019, vũ khí trong chiến dịch của Volodymyr Zelensky là mạng xã hội, nền tảng video và ứng dụng nhắn tin. Bản tin tối trên truyền hình phát sóng và trang nhất của các nhật báo toàn quốc không nằm trên sân khấu đó. Fedorov phụ trách mảng kỹ thuật số của chiến dịch này, và sau khi cuộc bầu cử kết thúc, ông bước vào chính phủ.

Không có tài liệu gốc nào cho thấy ông đã đưa ra quyết định gì bên trong chiến dịch, hoặc ông đã nói gì với ai, xuất hiện trong danh mục nguồn đã được bảo đảm. Viết thêm không khí của một phòng họp, hay một cảnh làm việc xuyên đêm, thì cũng dễ thôi, nhưng những câu viết theo cách ấy không thể gánh được sức nặng của nền móng. Điều có thể xác nhận là kết quả. Chính phủ mới lập ra một bộ dành riêng cho chuyển đổi số, và giám đốc kỹ thuật số của chiến dịch đã ngồi vào ghế lãnh đạo bộ đó.

Khi một bộ được thành lập và ngân sách được phân bổ cho bộ ấy, quyền yêu cầu các bộ khác làm việc cũng đi kèm, và một chuẩn đo kết quả được đặt ra. Những mục tiêu mà chính phủ Ukraine giao cho bộ này còn được lưu lại bằng văn bản: đưa dịch vụ công lên mạng trước năm 2024, đào tạo kỹ năng số cho hàng triệu công dân, mở rộng khả năng tiếp cận internet trên toàn quốc, và tăng tỷ trọng của công nghệ thông tin trong nền kinh tế.

Những gì có ở đây là các mục tiêu mà chính phủ Ukraine tự đặt ra cho mình, khác với các thành tựu đã được một cơ quan bên ngoài kiểm chứng. Mục tiêu của chính phủ, thông báo của chính phủ, và xác minh của bên thứ ba có trọng lượng khác nhau. Nếu đặt cả ba ngang hàng

bằng cùng một cỡ chữ, người đọc sẽ vô tình xem lời quảng bá như sự thật. Ranh giới này phải được áp dụng lại mỗi lần một con số phía sau xuất hiện.

Công nghệ số đã nằm ở trung tâm công việc của ông ngay từ đầu. Các báo cáo của nhiều tổ chức quốc tế và viện nghiên cứu lặp lại một chẩn đoán gần giống nhau. Bộ máy hành chính Ukraine trong nhiều năm dựa vào quầy dịch vụ, biểu mẫu giấy và người trung gian. Muốn lấy một giấy chứng nhận quyền sở hữu, người dân phải đến cơ quan nhà nước nhiều lần, rồi tự tay mang tờ giấy nhận ở quầy này sang quầy khác. Hàng chờ càng dài, thủ tục càng mờ, thì càng có nhiều chỗ cho một người bước vào và đề nghị giúp bạn bỏ qua hàng chờ ấy. Các báo cáo của Brookings Institution và Organisation for Economic Co-operation and Development (OECD) mô tả việc đưa dịch vụ lên mạng là giảm các điểm tiếp xúc trực tiếp giữa người với người, và ghi nhận logic rằng càng ít điểm tiếp xúc như vậy thì càng ít vai trò cho tiền được trao tay dưới gầm bàn. Stanford Social Innovation Review nhìn hành chính số của Ukraine không phải như một câu hỏi về hiệu quả hành chính, mà như một câu hỏi về niềm tin vào nhà nước. Ở một quốc gia nơi người dân không tin nhà nước của mình, thay đổi cách nhà nước và công dân gặp nhau vừa là một dự án kỹ thuật, vừa là một dự án chính trị.

Lời giải thích này vẫn chưa được kiểm chứng. Lập luận rằng việc xóa bỏ cửa tiếp dân giúp giảm tham nhũng là có lý. Nhưng khi cửa tiếp dân biến mất, cơ sở dữ liệu vẫn còn đó, và vài bàn tay quản lý cơ sở dữ liệu ấy cũng vẫn còn. Thay cho người từng giấu hồ sơ giấy, giờ có một người nắm quyền truy cập dữ liệu. Tham nhũng đã biến mất, hay chỉ chuyển sang một nơi khác nơi nó vẫn có thể xảy ra, đó là câu hỏi còn phải được xác nhận riêng.

Từ năm 2019, Fedorov lãnh đạo bộ này từ một vị trí đồng thời mang hàm phó thủ tướng. Chức danh "First Deputy Prime Minister" được gắn vào trong đợt cải tổ nội các tháng 7 năm 2025 và kéo dài cho đến khi ông trở thành bộ trưởng quốc phòng vào tháng 1 năm 2026. Vì việc bộ này định làm không kết thúc trong bốn bức tường của chính nó, cấp bậc chính là quyền lực. Bộ nội vụ nắm thông tin giấy phép lái xe và đăng ký phương tiện. Bộ tư pháp nắm giấy tờ sở hữu và hồ sơ khai sinh; cơ quan thuế nắm mã số người nộp thuế. Một tập hợp hồ sơ chính thức như vậy được gọi là "registry" trong ngôn ngữ hành chính. Có thể hình dung đó là một danh sách chính thức, được sắp theo từng loại, về những gì nhà nước biết về một công dân. Vấn đề là các registry này nằm trong những hệ thống khác nhau ở từng bộ, theo định dạng khác nhau, dưới những quy tắc khác nhau. Một số dùng cơ sở dữ liệu hiện hành; một số gần với sổ bộ cũ hơn. Muốn đưa một nhà nước lên một màn hình điện thoại thông minh, trước hết phải nối những thứ rải rác ấy lại với nhau, và muốn yêu cầu chúng được nối lại, người ta phải có quyền đưa ra yêu cầu đó.

Khó có thể gọi Diia là công trình của một người. Các báo cáo ghi nhận rằng tiền và hỗ trợ kỹ thuật từ các cơ quan tài trợ quốc tế, sự tham gia của các công ty phát triển tư nhân, và mô hình liên kết dữ liệu mà Estonia đã xây trước đó, tất cả đều được đặt chồng lên dự án này. Vị bộ

trưởng đặt nhịp ở giữa những tầng xếp đó; những bàn tay khác viết mã cho ứng dụng. Nếu gọi tên ông cho thật chính xác, nên nói là người lắp ghép, hoặc người thúc đẩy, hơn là nhà phát minh. Mọi đánh giá về một người thúc đẩy phải bao gồm cả thứ ông đã thúc đẩy và cả thứ ông đã đẩy lùi lại sau.

Sự tồn tại của một bộ không tự động kéo theo thẩm quyền. Mở một registry do bộ khác nắm giữ đồng nghĩa với việc sửa luật và các quy định thi hành, còn sửa luật nghĩa là phải thông qua một cuộc bỏ phiếu ở quốc hội. Tại Ministry of Digital Transformation, phần việc nhìn thấy được là ứng dụng, nhưng phần việc đòi hỏi đôi tay dài là lập pháp. Một trường hợp về sau cho thấy đặc điểm này. Vài ngày trước cuộc xâm lược toàn diện, quốc hội Ukraine thông qua một đạo luật về dịch vụ đám mây, cho phép dữ liệu cốt lõi của nhà nước được lưu trong các đám mây bên ngoài lãnh thổ quốc gia. Cho đến khi đạo luật ấy có hiệu lực, việc đặt dữ liệu nhà nước trên máy chủ nước ngoài là không hợp pháp. Một ứng dụng xuất hiện trên màn hình chỉ trong vài tháng; đạo luật làm nền cho nó thì di chuyển theo tốc độ của một lá phiếu.

Chính phủ phải thuyết phục các bộ khác và các công chức khác. Nhìn từ phía đang nắm dữ liệu, dữ liệu là quyền lực, và yêu cầu trao lại quyền lực không phải là điều dễ được đón nhận. Một vị trí đồng thời mang hàm phó thủ tướng là vị trí có thể thúc đẩy những yêu cầu như vậy đi đến cùng. Nhưng một quy tắc được áp đặt bằng sức mạnh và một quy tắc được xây dựng bằng đồng thuận sẽ để lại những hình dạng khác nhau. Khi người đã thúc đẩy nó rời khỏi vị trí, chính những quy tắc mà ông đã đẩy vào đời sống là những thứ đầu tiên lung lay. Không có tài liệu gốc nào ghi lại việc bộ này thực sự xử lý các cuộc va chạm giữa các bộ ra sao trong danh sách nguồn đã được bảo đảm, vì vậy ở đây không suy đoán điều gì.

Chuẩn mực dùng để đo kết quả cũng cần được xem xét kỹ. Chính phủ đặt mục tiêu đưa các dịch vụ lên trực tuyến vào năm 2024, rồi sau đó đưa ra tỷ lệ sử dụng và số lượng dịch vụ như bản báo cáo thành tích của mình. Con số 63 phần trăm, do Chương trình Phát triển Liên Hợp Quốc thu được vào năm 2023 bằng cách hỏi trực tiếp người dân, có sức nặng khác với một con số do chính phủ tự công bố về mình, vì bên đặt câu hỏi đứng ngoài chính phủ. Dù vậy, con số này cho chúng ta biết người dân dùng dịch vụ nhiều đến đâu, chứ không cho biết tiền lót tay có giảm tương ứng với mức cửa tiếp nhận hồ sơ biến mất hay không. Không có tài liệu nào đo từ bên ngoài xem tham nhũng có thực sự giảm hay không trong danh sách nguồn đã được bảo đảm.

Đánh giá kết quả cũng có nghĩa là nhìn vào tiền và công nghệ đến từ đâu. Các báo cáo ghi nhận rằng tiền từ các cơ quan tài trợ quốc tế, bàn tay của các công ty phát triển tư nhân, và mô hình mà Estonia xây dựng trước đó đã được xếp lớp lên dự án này. Một hệ thống được dựng bằng tiền bên ngoài và công nghệ bên ngoài phải có khả năng đứng vững vào ngày những thứ đó bị cắt đi. Về việc chính phủ Ukraine đã chuẩn bị cho ngày ấy ra sao, hồ sơ công khai dừng lại ở đây. Thành lập một bộ và làm cho một bộ có thể tự đứng vững là hai công việc khác nhau, và

hồ sơ công khai chỉ cho thấy công việc thứ nhất.

2. Diia và Trembita: Thiết kế nhà nước bên trong một chiếc điện thoại thông minh

Tháng 2 năm 2020, ứng dụng di động Diia được phát hành. Những giấy tờ đầu tiên mà ứng dụng này mang theo là giấy phép lái xe điện tử và giấy chứng nhận đăng ký xe. Việc từng có nghĩa là rút một tấm thẻ nhựa khỏi ví đã chuyển lên màn hình điện thoại thông minh. Một cổng web cũng mở ra trong cùng thời gian đó, và cấu trúc trong đó ứng dụng và cổng thông tin vận hành như một cặp đã được hình thành từ khi ấy.

Từ tiếng Ukraine "Diia" (Дія) có nghĩa là "hành động." Trên nền nghĩa này, ở Ukraine, người ta cũng đọc tên đó như một từ viết tắt của "Derzhava i ya" (Держава і я), nghĩa là "nhà nước và tôi." Hai cách giải thích này không loại trừ nhau, nhưng cũng không phải là cùng một sự thật: một bên là nghĩa của một từ, bên kia là lối chơi chữ được gắn thêm sau đó. Các phần giới thiệu bằng tiếng Hàn thường trộn lẫn hai điều này và viết, "Diia có nghĩa là 'nhà nước và tôi,'" một câu không khớp với nguyên gốc. Trông có vẻ là một lỗi nhỏ, nhưng thói quen chuyển cả một cái tên sang ngôn ngữ khác mà không kiểm tra nguồn sẽ lặp lại y hệt trong các con số và trích dẫn.

Để Diia hoạt động, phải có thứ gì đó nối các giấy tờ của các cơ quan nhà nước với nhau. Tên của hệ thống đường ống đó là Trembita. Trembita là một nền tảng trao đổi dữ liệu của chính phủ, liên kết các sổ đăng ký nhà nước vốn được các bộ và cơ quan nắm giữ riêng rẽ, cho phép chúng truyền dữ liệu qua lại theo những quy tắc cố định. Ukraine đã điều chỉnh họ mô hình liên kết dữ liệu X-Road, do Estonia xây dựng đầu tiên, cho phù hợp với hoàn cảnh của mình.

Cách Trembita vận hành khá dễ mô tả. Hãy giả sử mỗi bộ có một nhà kho để xếp chồng hồ sơ của mình. Theo cách cũ, công dân phải đến từng nhà kho, sao một giấy tờ, rồi mang nó sang nhà kho khác; công dân chính là người chuyển phát. Trembita đặt một hành lang có quy cách cố định giữa nhà kho này và nhà kho kia. Nhà kho nào được phép đưa ra giấy tờ nào trong điều kiện nào đều được quyết định trước, và mọi thứ đáp ứng quy cách sẽ tự động di chuyển. Giờ đây hệ thống di chuyển giấy tờ, còn Diia là màn hình được gắn ở cuối hành lang đó.

Luận điểm trung tâm trong thiết kế của Diia xuất phát từ cấu trúc này: bản thân ứng dụng Diia không tích trữ thông tin cá nhân của công dân. Cách giải thích là ứng dụng lấy thông tin từ sổ đăng ký gốc thông qua Trembita đúng vào lúc cần dùng và đưa lên màn hình; khi màn hình đóng lại, thông tin đó không ở lại trong ứng dụng. Fedorov gọi đây là cấu trúc "data in transit". Theo logic này, vì dữ liệu không tụ lại ở một nơi, việc đột nhập vào ứng dụng cũng không đem lại một đống dữ liệu để mang đi.

Đó là một thiết kế có sức thuyết phục, nhưng nguồn phải được ghi nhận chính xác. Cơ sở chính cho tuyên bố rằng ứng dụng không lưu trữ thông tin cá nhân là phần giải thích do chính phủ Ukraine và chính bộ trưởng phụ trách đưa ra. Trong hồ sơ công khai, không có báo cáo nào

từ một cơ quan bên ngoài đã kiểm toán độc lập mã nguồn hoặc cấu hình máy chủ của Diia. Ý đồ thiết kế và cách triển khai thực tế có thể khác nhau, và việc triển khai có đúng với ý đồ hay không chỉ thật sự có ý nghĩa khi được xác nhận từ bên ngoài bên đã xây dựng hệ thống. Hiện nay, điều có thể nói chỉ dừng ở mức "chính phủ Ukraine tuyên bố rằng họ đã thiết kế hệ thống theo cách này", còn những câu đi xa hơn đã được để ra ngoài phần chính của văn bản.

Các giấy tờ và dịch vụ được đưa vào ứng dụng tăng rất nhanh. Thẻ sinh viên điện tử, mã số người nộp thuế, đăng ký khai sinh, đăng ký kinh doanh và chứng nhận tiêm chủng bệnh truyền nhiễm lần lượt xuất hiện. Những việc trước đây cần phải đến quầy dịch vụ nếu muốn có bản giấy, từng việc một được chuyển lên màn hình. Năm 2021, chính phủ Ukraine giới thiệu hộ chiếu số có giá trị pháp lý ngang với hộ chiếu giấy và công bố đây là "world first". Cụm "world first" đó là tuyên bố của chính phủ Ukraine, và trong danh sách nguồn đã bảo đảm không có tài liệu độc lập nào so sánh từng điểm của nó với hệ thống của các nước khác. Cách nói như vậy rất mạnh trong nội dung quảng bá, nhưng khi được chuyển thành một phát biểu về sự thật, bên đưa ra tuyên bố phải được nêu tên cùng với nó.

Số người dùng Diia tăng nhanh. Trong một cuộc khảo sát do Chương trình Phát triển Liên Hợp Quốc (UNDP) thực hiện năm 2023, 63 phần trăm người Ukraine nói rằng họ dùng các dịch vụ điện tử của nhà nước. Các dịch vụ công có thể tiếp cận qua ứng dụng và cổng thông tin sau đó tăng lên khoảng 150. Cả hai con số đều là giá trị của vài năm sau khi ra mắt, và ở giữa đã xảy ra một cuộc xâm lược toàn diện. Điểm cuối của một đường tăng trưởng không được dùng làm bảng điểm cho điểm khởi đầu. Diia vào năm 2020 là một ứng dụng có giấy phép lái xe bên trong; 150 dịch vụ và 63 phần trăm là hình ảnh của ứng dụng đó sau khi đã lớn lên trong vài năm.

Nếu Diia là ứng dụng dành cho công dân, thì ở phía ngành công nghiệp, một cơ chế khác đã được đặt vào vị trí. Diia.City là một thiết chế pháp lý. Đó là một khu vực thể chế cho phép các công ty công nghệ thông tin hoạt động trong Ukraine theo các quy tắc riêng về thuế và hợp đồng; đạo luật tạo cơ sở cho nó được chuẩn bị vào năm 2021 và bắt đầu vận hành vào đầu năm 2022. Mục tiêu rất rõ. Thay vì để các lập trình viên phần mềm của Ukraine làm việc cho các pháp nhân nước ngoài hoặc rời khỏi đất nước, hãy khiến họ thành lập công ty ngay trong nước và nộp thuế tại đây. Giữ chân nhân tài của một quốc gia là công việc chậm hơn và ồn ào hơn so với việc xây thêm một ứng dụng, vì việc đó chạm tới các quy tắc thuế và lao động, và ngay khi chạm vào chúng, các lợi ích sẽ va vào nhau.

Diia là màn hình mà công dân sử dụng, Trembita là nền móng nối các tài liệu của các cơ quan nhà nước, còn Diia.City là thiết chế dành cho các công ty công nghệ thông tin. Nếu chỉ có màn hình thì không có dữ liệu để hiển thị, nếu chỉ có hệ thống đường ống thì công dân không có cách nào dùng nó, và nếu chỉ có thiết chế thì không có ai xây dựng bất cứ thứ gì.

The Brookings Institution chỉ ra rằng tổ hợp này đã vận hành ở một mức đáng kể trước chiến tranh, và coi đó là tiền đề cho sức chống chịu số của Ukraine. Những gì được xây trước chiến tranh chính là những gì được dùng trong chiến tranh. Phân tích từ Kennedy School của Harvard cũng không đọc trường hợp Ukraine như một câu chuyện trong đó khủng hoảng sinh ra đổi mới. Cách đọc của họ là năng lực đã được tích lũy trước khủng hoảng, rồi được khủng hoảng làm lộ ra. Nhiều câu văn đã kể vài ngày của tháng 2 năm 2022 theo giọng kịch tính, nhưng điều làm cho vài ngày ấy có thể xảy ra là mấy năm trước đó.

Các báo cáo ấy cũng gắn kèm những điều kiện. Organisation for Economic Co-operation and Development lưu ý rằng chuyển đổi số của Ukraine không vươn tới một cách đồng đều ở các vùng mà internet không chạm tới, tới người cao tuổi, hay tới các hộ gia đình thu nhập thấp. Không có điện thoại thông minh, bạn không thể bước vào nhà nước nằm trong điện thoại thông minh. Vấn đề này được giải bằng các lựa chọn chính trị: giữ lại bao nhiêu quầy dịch vụ trực tiếp, và chi bao nhiêu ngân sách cho những quầy được giữ lại. Chỉ công nghệ thì không giải được việc đó, và những thống kê khoe tốc độ chuyển dịch lên trực tuyến không nắm bắt tốt kết quả của lựa chọn ấy.

Họ cũng kiểm tra trước xem hệ thống có chịu được khi bị tấn công hay không. Trong một cuộc phỏng vấn, Bộ trưởng Fedorov nói rằng năm 2021, họ tập hợp các hacker đạo đức từ khắp thế giới và treo thưởng vài triệu hryvnia để thử đột nhập vào Diia. Hacker đạo đức là những người tấn công một hệ thống khi được cho phép, nhằm tìm ra điểm yếu của hệ thống đó. Theo ông, ba hoặc bốn tháng trước cuộc xâm lược, họ lập một đơn vị tấn công nội bộ trong chính phủ, gọi là "red team", rồi để đơn vị này liên tục đánh vào Diia, cổng thông tin chính phủ và ngành năng lượng không nghỉ ngày nào. Nguồn của phát biểu này là chính cuộc phỏng vấn của bộ trưởng, và trong các tài liệu công khai đã được bảo đảm không có báo cáo bên ngoài nào ghi riêng kết quả của cuộc kiểm thử đó. Tự tấn công mình và được kiểm toán từ bên ngoài là hai việc khác nhau. Việc thứ nhất cho phép bên xây dựng tự quyết định mình sẽ tìm thấy gì; việc thứ hai tìm ra cả những điều bên xây dựng muốn giấu.

Việc lưu dữ liệu ở đâu cũng được quyết định trong giai đoạn này. Luật về dịch vụ đám mây, được thông qua ngay trước cuộc xâm lược toàn diện, đã mở đường cho việc lưu dữ liệu cốt lõi của nhà nước trên các đám mây ở nước ngoài. Đưa máy chủ ra khỏi lãnh thổ quốc gia có nghĩa là tránh được bom đạn, đồng thời cũng có nghĩa là chuyển sang phạm vi luật pháp của một quốc gia khác và điều khoản dịch vụ doanh nghiệp của một quốc gia khác. Trong danh sách nguồn đã được bảo đảm, không thấy tài liệu nào cho biết hợp đồng nào đã đặt ra các điều kiện đó. Cái giá của một cấu trúc như vậy, màn hình và hệ thống đường ống được xây trong nước, còn dữ liệu được gửi vào kho của một công ty nước ngoài, vẫn là chuyện chỉ có thể tranh luận trên giấy cho đến khi hóa đơn thật sự đến hạn.

Tác động của Diia.City phải được kiểm chứng riêng. Khu vực này, nơi áp dụng các quy định thuế và hợp đồng khác cho các công ty công nghệ thông tin, là một công cụ để giữ các nhà phát triển ở lại trong nước. Nhưng một hệ thống cắt giảm thuế cũng có nghĩa là ngân khố mất đi đúng phần tiền đã được cắt giảm. Số tiền đó lớn hơn hay nhỏ hơn giá trị của lượng nhân tài được giữ lại là phép tính phải được làm riêng. Trong hồ sơ công khai, không có số liệu thống kê độc lập nào đo lường thiết chế này đã ngăn được bao nhiêu nhà phát triển rời đi. Ghi nhận mục đích của một thiết chế và xác nhận tác động của một thiết chế là hai công việc khác nhau.

3. Vai trò nơi tiện lợi, an ninh và nỗi lo bị giám sát va chạm

Một dịch vụ càng tiện lợi, càng nhiều thông tin di chuyển bên trong cùng một hệ thống. Diia cũng không khác. Nói rằng giấy phép lái xe, mã số thuế, hồ sơ khai sinh và đăng ký kinh doanh của một người có thể được truy cập qua một màn hình duy nhất cũng có nghĩa là ai nắm chìa khóa của màn hình ấy có thể nhìn thấy toàn bộ nội dung đời sống của người đó.

Những lo ngại về an ninh được nêu ra trước tiên. Cơ quan truyền thông công dân quốc tế Global Voices, trong bài viết có nhan đề "Security concerns and legal ambiguity threaten the future of Ukraine's 'state in a smartphone,'" đã chỉ ra các lỗ hổng và khoảng trống pháp lý phát sinh khi dữ liệu của công dân được gom vào một hệ thống duy nhất. Chính phủ Ukraine trả lời bằng lập luận "ứng dụng không lưu dữ liệu" đã nói ở trên. Nhưng trọng tâm phê phán nằm ở các sổ đăng ký phía sau ứng dụng, và những hành lang nối các sổ đăng ký ấy với nhau. Hành lang giữa các kho càng được khoan thông suốt, thì khi một kho riêng lẻ bị mở, càng nhiều thứ khác cũng mở theo.

Những lo ngại ấy đã có tiền lệ. Năm 2018, có thông tin cho rằng dữ liệu cá nhân của 500.000 khách hàng của Nova Poshta, một công ty logistics lớn của Ukraine, đã bị rò rỉ lên dark web. Dark web là vùng của internet mà công cụ tìm kiếm thông thường không chạm tới được, người truy cập che giấu danh tính, và bên trong đó có những chợ mua bán dữ liệu cá nhân bị đánh cắp. Đây là sự cố tại một công ty tư nhân, nhưng trong xã hội Ukraine nó được nhắc đến như một trường hợp cho thấy khối lượng lớn dữ liệu cá nhân thoát ra ngoài bằng con đường nào và được giao dịch ở đâu.

Vài năm sau, vào năm 2023, Ngân hàng Quốc gia Ukraine (NBU) công bố rằng thiệt hại do gian lận tài chính đã tăng 73 phần trăm so với năm trước. Con số này là thống kê riêng của ngân hàng trung ương, và khác với một giá trị được tính bằng cách chỉ tách riêng các thiệt hại do lỗi trong Diia gây ra. Có thể đặt hai sự kiện cạnh nhau, nhưng không được đọc sự kiện này như nguyên nhân của sự kiện kia. Có thể rút ra mối liên hệ theo lẽ thường rằng gian lận sẽ dễ hơn trong một xã hội nơi nhiều dữ liệu cá nhân trôi nổi trên thị trường, nhưng trong danh sách nguồn đã được bảo đảm không thấy tài liệu nào xác lập mối liên hệ đó như quan hệ nhân quả.

Cùng với vấn đề an ninh, câu hỏi về giám sát ngày càng lớn hơn. Năm 2019, thủ đô Kyiv xuất hiện trong kết quả một khảo sát, được xếp vào nhóm năm mươi thành phố trên thế giới có mật độ camera giám sát cao nhất. Các thành phố của Ukraine mở rộng mạng lưới camera dưới tên gọi "Safe City", và công nghệ nhận diện khuôn mặt bắt đầu được đặt chồng lên trên. Nhận diện khuôn mặt là công nghệ đối chiếu khuôn mặt được camera ghi lại với một danh sách ảnh đã lưu, rồi tự động phán đoán người đó là ai. Khác với con người phải nhìn từng hình ảnh trên màn hình, máy móc không mệt và kiểm tra mọi khuôn mặt. Viện nghiên cứu xã hội Ukraine Cedos, trong báo cáo có nhan đề "Surveillance cameras and the municipal guard. How safe is the 'Safe City'?", nhận xét rằng sự mở rộng này có thể làm nguội lạnh tự do của công dân, còn các nhà hoạt động thì ví nó với tiểu thuyết của George Orwell, gọi đó là "con mắt sắc bén của Big Brother".

Việc lắp thêm camera và việc xây dựng một ứng dụng là hai công việc riêng, do các bộ khác nhau phụ trách. Trong hồ sơ công khai, không có căn cứ để nói rằng Ministry of Digital Transformation đã chỉ đạo việc mở rộng các mạng lưới giám sát đô thị. Nhưng trong mắt người dân, chúng trông như đang đi cùng một hướng, vì dòng chảy chung là nhà nước có thể nhận diện công dân kỹ hơn, ghi lại nhiều dữ liệu hơn về họ, và nối các hồ sơ đó với nhau nhanh hơn. Việc bộ tạo ra sự tiện lợi và bộ bổ sung giám sát là hai cơ quan khác nhau có ý nghĩa về mặt hành chính, nhưng điều đó không an ủi được người dân phải gánh kết quả.

Các nhà sản xuất camera giám sát cũng trở thành một vấn đề gây tranh cãi. Một tỷ lệ đáng kể camera giám sát được lắp đặt trên khắp Ukraine là sản phẩm của hai công ty Trung Quốc Hikvision và Dahua. Năm 2023, Kyiv Post đăng một bài bình luận có nhan đề "Trojan Horse: How Chinese Cameras Put Ukraine at Risk", cảnh báo rằng phần cứng nằm trong phạm vi ảnh hưởng của một chính phủ nước ngoài có thể trở thành cửa hậu đi vào mạng lưới giám sát của Ukraine. Bài viết đó gần với ý kiến bình luận hơn. Trong danh sách nguồn đã được bảo đảm, không thấy có phóng sự điều tra nào xác nhận về mặt kỹ thuật rằng một cửa hậu đã thật sự mở ra và có dữ liệu đi ra qua đó; cảnh báo và bằng chứng có sức nặng khác nhau.

Quốc hội cũng bắt đầu chuẩn bị luật để bảo vệ dữ liệu cá nhân. Một dự luật bảo vệ dữ liệu cá nhân (dự thảo số 8153), đi theo tiêu chuẩn của General Data Protection Regulation (GDPR) của European Union, đã được trình lên quốc hội Ukraine vào tháng 10 năm 2022. GDPR là luật châu Âu quy định ai được lưu giữ dữ liệu cá nhân, vì mục đích gì, trong bao lâu, và trao cho công dân quyền yêu cầu được tiếp cận và xóa dữ liệu. Council of Europe đã triệu tập một cuộc thảo luận chuyên gia và nêu rõ rằng khi quyền thu thập dữ liệu của nhà nước được mở rộng trong điều kiện ngoại lệ của chiến tranh, cần có các hàng rào pháp lý để bảo vệ công dân.

Ngày được đưa ra là tháng 10 năm 2022. Hai năm rưỡi đã trôi qua kể từ khi Diia ra đời, và tám tháng kể từ khi cuộc xâm lược toàn diện bắt đầu. Tốc độ tạo ra sự tiện lợi và tốc độ đặt ra các quy tắc để quản lý sự tiện lợi đó không giống nhau. Ứng dụng xuất hiện chỉ trong vài tháng;

luật để quản lý dữ liệu mà ứng dụng ấy xử lý thì nhiều năm sau mới bắt đầu được bàn thảo. Độ trễ này cũng lặp lại ở các nước khác, nhưng ở Ukraine, độ trễ ấy chồng lên một cuộc chiến.

Những câu hỏi nằm ngoài hồ sơ công khai vẫn còn đó. Chúng tôi không thể có được một báo cáo gốc từ các tổ chức nhân quyền hoặc nhóm xã hội dân sự của Ukraine trực tiếp điều tra cách Diia xử lý dữ liệu. Một phần lớn các lời phê bình đến với chúng ta qua các bản tóm tắt của truyền thông nước ngoài hoặc qua các văn bản phản bác do bộ phụ trách ban hành. Một cấu trúc trong đó phê bình chỉ được đọc qua phản bác là cấu trúc nguy hiểm. Một bản phản bác có thể chọn trong nhiều lời phê bình những điểm dễ bác bỏ nhất để trích dẫn, rồi bỏ qua những điểm khó xử. Viết rằng chúng tôi không thể lấp đầy khoảng trống ấy thì tốt hơn là viết như thể không hề có khoảng trống nào.

Từ năm 2019 đến đầu năm 2022, Ukraine đã đưa nền hành chính của mình vào điện thoại thông minh với một tốc độ mà rất ít quốc gia trên thế giới sánh kịp. Màn hình, hạ tầng kỹ thuật và thiết chế được xây dựng cùng lúc, và người dân không còn phải xếp hàng trước quầy dịch vụ. Trong cùng giai đoạn đó, dữ liệu chống đỡ cho sự tiện lợi ấy được nối với nhau chặt hơn, camera trong các thành phố tăng lên, còn luật để xử lý tất cả những điều đó chỉ bắt đầu được bàn thảo muộn. Thành tựu và lo ngại không phải là hai sự kiện tách rời, mà là hai mặt của cùng một sự kiện.

Trước chiến tranh, tiện lợi, an ninh và giám sát là ba lực kéo về ba hướng khác nhau. Ba lực ấy cuối cùng sẽ cân bằng ra sao vẫn chưa được quyết định, và việc quyết định thế cân bằng đó là công việc của luật pháp và chính trị. Ngày 24 tháng 2 năm 2022, một trong ba lực ấy đã lấn át hai lực còn lại, vì sự sống còn của nhà nước được đặt lên trước mọi cuộc bàn luận khác.

Các nước khác đã vạch sẵn ranh giới về nguồn gốc của những camera này. Ủy ban Truyền thông Liên bang Hoa Kỳ chặn nhập khẩu thiết bị Hikvision và Dahua vì lo ngại gián điệp, còn Nghị viện châu Âu gỡ bỏ thiết bị Hikvision với lý do liên quan đến vi phạm nhân quyền. Sau đó, các thành phố của Ukraine vẫn tiếp tục dùng camera của những công ty này. Hồ sơ công khai dừng lại ở câu hỏi vì sao họ vẫn dùng. Không có hồ sơ điều tra nào đủ để phân biệt đó là vì giá thấp, vì không có ngân sách mua thiết bị thay thế, hay vì có chuyện khác trong khâu mua sắm công. Viết phần nằm ngoài hồ sơ công khai như thể đã được xác nhận thì câu văn sẽ trở thành lời cáo buộc, mà cáo buộc thì cần chứng cứ.

Nhận diện khuôn mặt đã vượt khỏi phạm vi tiện lợi hành chính để trở thành một công cụ chiến tranh. Chính phủ Ukraine đưa phần mềm nhận diện khuôn mặt của công ty Mỹ Clearview AI vào hoạt động quân sự. Cách dùng được tường thuật như sau: chụp ảnh khuôn mặt một binh sĩ Nga tử trận, đối chiếu với đống ảnh trôi nổi trên internet để biết danh tính người đó, rồi báo tin cho mẹ của binh sĩ ấy ở Nga rằng con bà đã chết. Công ty này đã bị cấm hoặc bị phạt tại ít nhất bốn quốc gia thành viên Liên minh châu Âu vì vấn đề thu thập hàng tỷ ảnh khuôn mặt từ internet mà không xin phép. Digital Security Lab của Ukraine lưu ý rằng trong luật Ukraine

không tồn tại khuôn khổ pháp lý nào điều chỉnh việc dùng công nghệ này trong quân sự.

Khi quyền lực của cơ quan phụ trách giám sát và an ninh lớn lên, câu hỏi tiếp theo là ai giám sát cơ quan đó. Tháng 7 năm 2023, Ukrainian League of Industrialists and Entrepreneurs phê phán dự luật an ninh mạng số 8087 vì tập trung quá nhiều thẩm quyền vào State Service of Special Communications and Information Protection. Không lâu sau, National Anti-Corruption Bureau của Ukraine thông báo rằng hai nhân vật cấp cao của cơ quan này, trong đó có người đứng đầu Yurii Shchyhol, bị nghi rút ruột 62 triệu hryvnia trong quá trình mua phần mềm; hai người rời chức vụ và bị điều tra. Luận điểm ở phần đầu, rằng bỏ cửa sổ dịch vụ sẽ giảm tham nhũng, quay lại ở đây. Những cửa sổ giấy đã thu hẹp lại, nhưng cửa sổ mua sắm vẫn còn nguyên.

Tháng 11 năm 2023, chính phủ Ukraine tham dự AI Safety Summit tổ chức tại Anh và ký Bletchley Declaration. Một chữ ký là một lời hứa, còn lời hứa không phải là quy tắc. Biến lời hứa thành quy tắc là việc của quốc hội và tòa án, và như chúng ta đã thấy, việc đó bắt đầu muộn.

Chương 2. Tháng 2 năm 2022: Chính phủ điện tử trở thành hạ tầng thời chiến

Ngày 23 tháng 2 năm 2022, một làn sóng khổng lồ các nỗ lực kết nối ập vào mạng lưới của chính phủ Ukraine. Các cổng thông tin chính phủ và trang ngân hàng chao đảo. Vô số máy tính cùng lúc cố gắng kết nối để làm máy chủ ngừng hoạt động, phương thức mà ngành an ninh gọi là tấn công DDoS. Cùng thời điểm đó, một loại chương trình khác bắt đầu chạy trên một số hệ thống. Đó là phần mềm độc hại được tạo ra để xóa tệp đến mức không còn hy vọng khôi phục, và ngành an ninh gọi loại này là wiper. Những mẫu được phát hiện hôm đó được đặt tên là HermeticWiper và FoxBlade. Một số báo cáo phân tích quy cuộc tấn công cho Sandworm, một nhóm tin tặc được xác định là có liên hệ với cơ quan tình báo quân sự của Nga, GRU. Và vào rạng sáng hôm sau, lực lượng mặt đất vượt qua biên giới.

Chính phủ điện tử của Ukraine bị tấn công vào tháng 2 năm 2022 nhưng vẫn tiếp tục hoạt động. Tuy vậy, phần lớn tài liệu công khai làm căn cứ cho nhận định đó lại là các thông báo từ chính chính phủ Ukraine. Chỉ khi tách các tuyên bố của chính phủ khỏi việc kiểm chứng của các cơ quan bên ngoài, chúng ta mới có thể nhìn rõ Diia thực sự đã đóng vai trò gì trong cuộc chiến.

1. Nền hành chính số không bao giờ tắt, ngay cả trong ngày đầu tiên

Vài ngày trước khi chiến tranh bắt đầu, quốc hội Ukraine đã thông qua một đạo luật cho phép dữ liệu cốt lõi của nhà nước được lưu trữ trên các đám mây ở nước ngoài.

Trước thay đổi đó, hồ sơ nhà nước không thể được lưu giữ bên ngoài Ukraine. Cho đến lúc ấy, luật Ukraine vẫn buộc các cơ sở đăng ký quốc gia, từ quyền sở hữu đất đai đến hồ sơ cư trú, phải nằm trên máy chủ đặt trong nước. Cách nghĩ khi đó là dữ liệu phải ở trong biên giới thì nhà nước mới kiểm soát được, và trong thời bình, logic ấy nghe có vẻ hợp lý. Nhưng trong thời chiến, ý nghĩa đổi khác. Nói rằng một máy chủ nằm trong nước cũng có nghĩa là máy chủ ấy trở thành một tọa độ trên bản đồ, và một quả bom rơi vào một tòa nhà có thể xóa sạch hồ sơ tài sản của cả một quốc gia chỉ trong một đòn.

Đám mây nghĩa là các trung tâm dữ liệu của người khác, rải khắp thế giới. Bạn đặt tài liệu của mình trên các máy chủ trong những tòa nhà do các công ty như Amazon hay Microsoft vận hành, rồi lấy lại chúng qua internet. Nếu một tòa nhà bị phá hủy mà một bản sao giống hệt vẫn còn ở nơi khác, tài liệu sẽ sống sót. Điều Ukraine thay đổi ngay trước thềm cuộc xâm lược là luật pháp. Công nghệ ấy đã tồn tại trên thế giới; thứ còn thiếu chỉ là sự cho phép, và một khi sự cho phép xuất hiện, việc di chuyển dữ liệu vẫn còn phải được thực hiện.

Khối lượng dữ liệu khổng lồ cũng là một vấn đề. Hồ sơ quốc gia được đo bằng petabyte (PB). Một petabyte xấp xỉ một triệu gigabyte. Một điện thoại thông minh chứa khoảng 128 gigabyte, nên một petabyte có thể lấp đầy hàng nghìn chiếc điện thoại như vậy đến tận giới hạn. Ngay từ

đầu, việc gửi chừng ấy tài liệu lên qua các đường truyền internet của một đất nước vừa bước vào chiến tranh đã là điều bất khả thi.

Amazon Web Services (AWS) đưa vào Ukraine một thiết bị gọi là Snowball. Đó là một bộ lưu trữ dung lượng lớn, chịu va đập tốt, trông giống một chiếc vali. Tài liệu được nạp vào thiết bị này, được mang ra khỏi biên giới bằng đường vật lý, rồi được tải lên đám mây từ một trung tâm dữ liệu ở châu Âu. Nếu khối lượng quá lớn để gửi qua dây mạng, ý tưởng là đặt nó lên xe tải và chở qua biên giới. Nhiều báo cáo ghi nhận rằng chiến dịch này đã đưa khoảng 10 đến 15 petabyte tài liệu ra khỏi đất nước trong khoảng mười tuần, bao gồm sổ đăng ký đất đai, giấy tờ quyền sở hữu tài sản và hồ sơ ngân hàng. Các nguồn khác mô tả cùng chiến dịch này là cuộc giải cứu hơn mười triệu gigabyte dữ liệu của chính phủ và nền kinh tế. Hai con số ấy không chỉ hai sự kiện khác nhau; chúng nói về cùng một quy mô bằng hai đơn vị khác nhau.

Microsoft đã giúp các dịch vụ của chính phủ Ukraine có thể vận hành trên đám mây riêng của mình, Azure, và thông báo rằng công ty đã cung cấp miễn phí 400 triệu đô la tín dụng sử dụng đám mây. Con số này và nội dung cụ thể đến từ chính công bố của công ty; trong các tài liệu được tập hợp ở đây, không thấy có văn bản nào xác minh độc lập rằng số tín dụng đó thực tế đã được chi tiêu ra sao. Fedorov nói về công việc này: "Bạn không thể ném bom đám mây." Ý ông là việc phân tán hồ sơ quốc gia trên các máy chủ đặt tại lãnh thổ các nước thành viên NATO tự thân đã là một biện pháp răn đe.

Cách nói đó cần được xem xét về phạm vi của nó, thay vì chấp nhận nguyên xi. Có thể bạn không ném bom được đám mây, nhưng bạn có thể ném bom các mạng lưới liên lạc và điện lực dẫn tới nó, và nếu máy chủ vẫn sống mà đường truyền bị cắt, một công dân cũng không thể mở nổi một trang nào trong đó. Một bóng dài hơn nằm ở nơi khác. Đặt hồ sơ của một quốc gia trên máy chủ của các công ty tư nhân nước ngoài cũng có nghĩa là đặt ký ức của quốc gia ấy lên trên điều khoản dịch vụ của các công ty đó và luật pháp của những nước mà họ thuộc về. Nếu công ty thay đổi chính sách, ký ức của quốc gia khi ấy sẽ đứng ở đâu? Nhớ lại Starlink, câu hỏi này trở lại dưới một dạng sắc hơn nhiều.

Một thông báo rằng tài liệu đã được chuyển đi tự nó không giải quyết được việc quyền kiểm soát đối với chúng đã được sắp xếp ra sao, và đến nay vẫn chưa có câu trả lời nào xuất hiện. Chưa có hợp đồng nào được công khai cho thấy ai nắm giữ khóa mã hóa, liệu nhân viên tại các trung tâm dữ liệu nước ngoài có thể tiếp cận bản gốc hay không, hoặc liệu các cơ quan Ukraine có thể tự xóa các bản sao hay không. Thành tựu dữ liệu sống sót và câu hỏi ai kiểm soát dữ liệu đó là hai việc riêng biệt. Trong chiến tranh, việc thứ nhất là cấp bách; khi chiến tranh kết thúc, việc thứ hai vẫn còn đó.

Ngay sau cuộc xâm lược, chính phủ Ukraine đã tạm thời đóng một số dịch vụ. Chính họ đã cắt quyền truy cập từ bên ngoài vào một số sổ đăng ký quốc gia. Để ngăn kẻ thù trích xuất hoặc xóa tài liệu, khóa cửa an toàn hơn là để cửa mở, và cái giá là trong một thời gian, nhiều công

dân không thể mở giấy tờ điện tử của mình trong Diia.

Khi chiến tranh bắt đầu, chính phủ đã tạm dừng một số dịch vụ đang có trước khi đưa ra bất kỳ dịch vụ mới nào. Quyết định bảo vệ tài liệu của nhà nước lập tức trở thành một sự bất tiện đối với người dân, và chỉ trong một ngày, chiến tranh đã phơi bày sự thật rằng an toàn và tiện lợi không đi cùng một hướng.

Theo các tài liệu công khai, hoạt động hành chính cơ bản vẫn tiếp tục trong suốt chiến tranh. Qua nhiều tuần mất điện và tên lửa rơi xuống, các hoạt động hành chính nhìn chung vẫn được duy trì, hệ thống ngân hàng tiếp tục vận hành, và việc chi trả lương cùng lương hưu chưa bao giờ dừng lại. Việc một phần đáng kể của nhận định này lặp lại chính các phát biểu của Fedorov cần được đặt đúng vị trí của nó. Hồi ức của vị bộ trưởng phụ trách là lời chứng về các sự kiện, và chúng có trọng lượng khác với những kết luận đã được một cuộc kiểm toán bên ngoài xác nhận.

Lý do bản thân ứng dụng Diia chưa từng bị xâm nhập thường được cho là nằm ở thiết kế của nó. Diia không lưu dữ liệu cá nhân của công dân trên điện thoại, cũng không lưu trên máy chủ của ứng dụng. Thông qua Trembita, kênh trao đổi dữ liệu giữa các bộ, ứng dụng lấy thông tin từ các sổ đăng ký gốc mỗi khi cần, hiển thị lên màn hình, rồi không để lại gì sau khi màn hình đóng lại. Các tài liệu gọi đây là kiến trúc "data in transition". Điều đó có nghĩa là ngay cả khi đột nhập được vào ứng dụng, bên trong cũng không có gì để lấy.

Thiết kế này được tạo ra trong thời bình. An ninh là một phần của suy nghĩ ban đầu, nhưng mục tiêu lớn hơn là tránh kiểu hành chính cũ, nơi mỗi bộ tự chất đống tài liệu riêng của mình. Khi chiến tranh xảy ra, cùng một cấu trúc ấy mang một giá trị khác. Một ứng dụng không có gì để đánh cắp thì khi bị tấn công cũng không mất gì. Một nguyên tắc thiết kế thời bình đã trở thành tuyến phòng thủ thời chiến, và một phần đáng kể những gì Ukraine làm được trong năm 2022 diễn ra trên nền móng chính phủ điện tử đã được xây dựng qua nhiều năm kể từ 2019.

Một số vai trò không thể xác định chắc chắn. Chúng tôi không thể xác lập được các tài liệu cho thấy Ukraine đã thực hiện những cuộc kiểm tra an ninh nào trước cuộc xâm lược, hoặc nước này đã lập bản đồ trước các điểm yếu trong hệ thống chính phủ đến mức nào. Tài liệu được tập hợp ở đây cũng không có bất kỳ báo cáo kiểm toán nào đã được kiểm chứng từ bên ngoài về việc có bao nhiêu cuộc tấn công nhắm vào Diia sau cuộc xâm lược, hoặc liệu dữ liệu cá nhân có bị rò rỉ hay không. Một cách giải thích về cấu trúc rằng thiết kế làm giảm nguy cơ rò rỉ và một tuyên bố rằng số vụ rò rỉ trên thực tế là bằng không không thể được xem là có trọng lượng ngang nhau. Câu thứ nhất tồn tại trong các tài liệu công khai; câu thứ hai thì không.

Đây là điều có thể xác nhận về tháng 2 năm 2022. Nga cố làm tê liệt nhà nước bằng cách đánh vào các tòa nhà hành chính, hệ thống liên lạc và điện lực, còn Ukraine chuyển bộ máy hành chính ra khỏi các tòa nhà, lên các máy chủ bên ngoài biên giới. Một số báo cáo ghi nhận rằng phản ứng này đã có tác dụng. Việc phần lớn các tiếng nói mà những báo cáo đó trích dẫn

thuộc về chính phủ Ukraine cũng cần được đặt cùng chỗ với nhận định ấy.

Đằng sau khả năng chuyển hồ sơ quốc gia qua biên giới vào tháng 2 năm 2022 là một trình tự thời gian kéo dài trong nhiều năm trước đó. Chính phủ điện tử của Ukraine không lớn lên thong thả trong thời bình yên. Nó bắt đầu sau cuộc cách mạng Maidan năm 2014 với việc mở Prozorro, một nền tảng mua sắm công nhằm chống tham nhũng; rồi đến năm 2019, Ministry of Digital Transformation được thành lập, đưa vào Trembita và Vulyk, những kênh kết nối tài liệu giữa các bộ. Năm 2020, ứng dụng và cổng Diia, Diia.Business dành cho doanh nghiệp nhỏ và vừa, cùng một hệ thống chi trả hỗ trợ COVID-19 lần lượt được mở, và đầu năm 2022, ngay trước cuộc xâm lược, Diia City, một chế độ thuế dành cho các công ty công nghệ thông tin, được khởi động. Thứ đối mặt với chiến tranh không phải là một ứng dụng được dựng vội, mà là hệ thống đường ống đã kịp đông cứng.

Trước khi các tài liệu có thể được chuyển đi, cần có một nền tảng pháp lý, tức tư cách để nói: "hãy chuyển chúng đi." Cơ quan chính phủ điện tử được lập năm 2014 có thể hợp tác với từng bộ, nhưng không có thẩm quyền buộc họ tuân thủ. Năm 2019, công việc đó được chuyển sang Ministry of Digital Transformation mới thành lập, và đến năm 2023, bộ này đã tăng lên hơn 300 người. Bộ không trực tiếp xây dựng dịch vụ của các bộ khác. Bộ quản lý Trembita và Diia trong khi đứng ở vị trí giám sát, điều phối các dự án số trên toàn bộ chính phủ. Quốc hội cũng có một Committee on Digital Transformation hỗ trợ công việc này. Quyết định chuyển toàn bộ hồ sơ của một quốc gia lên các máy chủ bên ngoài biên giới trước hết là vấn đề thẩm quyền, rồi mới là vấn đề công nghệ, và cánh cửa để ban hành mệnh lệnh đó đã được mở từ ba năm trước cuộc xâm lược.

Không có nhiều thông tin về những phán đoán của các bên ở phía bên kia bàn đàm phán. Không tài liệu nào trong phần tư liệu được xem xét ở đây cho thấy vì sao Amazon và Microsoft quyết định chuyển giao thiết bị và tín dụng dịch vụ, hoặc những cuộc thảo luận nào bên trong các công ty đó đã dẫn đến quyết định ấy. Hai doanh nghiệp này đã đưa hồ sơ quốc gia của một đất nước đang có chiến tranh vào chính các tòa nhà của mình, và những hồ sơ đó đến nay vẫn ở đó. Chúng tôi không thể có được tài liệu xác nhận các điều khoản hợp đồng đi kèm là gì, việc lưu trữ sẽ kéo dài bao lâu, hoặc các tài liệu sẽ được trả về đâu khi chiến tranh kết thúc. Thiện chí của một công ty không phải là hợp đồng, và thiện chí không có hợp đồng có thể bị rút lại bất cứ lúc nào.

2. eVorog và báo cáo của công dân: cuộc chiến trong đó dân thường trở thành cảm biến

Tháng 3 năm 2022, một tháng sau cuộc xâm lược, một chatbot xuất hiện trên Telegram, ứng dụng nhắn tin mà người Ukraina dùng hằng ngày. Tên của nó là eVorog (єВорог), trong tiếng Anh là eEnemy, nếu diễn đạt thẳng ra là "kẻ thù điện tử". Chatbot là một kênh nơi chương trình tự động xử lý cuộc trò chuyện. Nếu người dân nhìn thấy binh sĩ, thiết bị hoặc đoàn xe của Nga,

họ có thể gửi ảnh có gắn vị trí địa lý, video và một mô tả ngắn vào kênh này, và dữ liệu gửi đến sẽ được chuyển tiếp sang các kênh tình báo quân sự để phân tích.

Việc Ukraina làm là nối một thiết bị vốn đã nằm trong túi của mọi người vào một kênh duy nhất. Không cần vũ khí mới, cũng không cần đơn vị mới. Lỗ hổng trong mối nối đó lộ ra ngay. Nếu ai cũng có thể gửi, kẻ thù cũng có thể gửi. Họ có thể làm ngập hệ thống bằng tọa độ giả và khiến pháo binh bên mình bắn nhầm chỗ; họ có thể đổ vào đó các báo cáo vô dụng và làm tê liệt những người đang kiểm chứng. Một hệ thống mở rộng cửa cho thông tin thì cũng mở rộng cửa như vậy cho thông tin sai lệch.

Ngay cả một báo cáo đã vượt qua bước xác thực cũng không chắc là chính xác. Con mắt của một thường dân khác với con mắt của một nhà phân tích quân sự. Không có lý do gì để tin rằng loại xe tăng và số lượng xe tăng nhìn thoáng qua giữa khói, tiếng ồn và nỗi sợ lại nhất định đúng. Một người hoảng sợ có thể đếm quá lên; người quan sát từ xa có thể nhầm loại này với loại khác. Vì vậy phải có một quy trình lọc. Các tài liệu ghi rằng những báo cáo đã được kiểm chứng của công dân, cùng với thông tin từ drone, vệ tinh và trinh sát, được đưa vào một hệ thống gọi là DELTA. DELTA là một nền tảng nhận thức chiến trường, xếp chồng thông tin đến từ nhiều nơi lên một bản đồ số duy nhất và cho chỉ huy thấy bức tranh tình hình theo thời gian thực. Có một sự kiện đáng giữ lại. Vào mùa xuân năm 2022, một mạch nối đã được dựng lên, qua đó điện thoại thông minh của một thường dân có thể đặt một dấu chấm lên bản đồ của quân đội.

Quy trình ra quyết định rất khó xác nhận chỉ bằng các tài liệu công khai. Chúng tôi không xác lập được tài liệu công khai cho biết danh tính của người báo tin được kiểm tra ra sao, bao nhiêu phần trăm báo cáo gửi đến dùng được, hoặc việc xác minh đi qua bao nhiêu bước và ai là người quyết định. Có dấu vết cho thấy những con số như vậy từng được nhắc đến dưới dạng phỏng vấn, nhưng chúng không được xác lập thành nguồn có thể trích dẫn, nên không được ghi như sự thật. Điều các tài liệu nói, rằng đã có một quy trình, là giới hạn xa nhất mà chúng ta có thể đi tới; quy trình ấy lọc kỹ đến mức nào thì nằm ngoài phạm vi xác nhận.

Quy mô không hề nhỏ. Một thống kê cho rằng tính đến cuối năm 2022, hơn 433.000 người Ukraine đã gửi thông tin chiến trường qua chatbot eVorog. Trong cùng thời gian, một kênh Telegram có tên "STOP Russian War" đã thu thập hơn 100.000 báo cáo về hoạt động di chuyển của đối phương. Con số 433.000 ấy là số công dân đã dùng một kênh báo cáo, và nó đến từ một hệ thống khác với số người tham gia IT Army, tức là một con số hoàn toàn khác. Không được đọc hai con số này như thể chúng chồng lên nhau.

Những con số này chứng minh điều gì cũng phải nói thật cẩn trọng. 433.000 là số người đã gửi báo cáo. Nó không chứa số người đã tạo ra một mục tiêu hợp lệ. Trong phạm vi tài liệu công khai được xem xét ở đây, không có tài liệu nào tự mình xác lập được các báo cáo của công dân thực tế đã dẫn đến bao nhiêu cuộc tấn công, hay các cuộc tấn công ấy đã góp phần thế nào vào

hình dạng của mặt trận. Quy mô tham gia được xác nhận; còn về kết quả, hồ sơ công khai dừng lại ở đây. Ngay khi ranh giới đó bị xóa đi, hồ sơ sẽ biến thành tuyên truyền.

Ở nước ngoài, tốc độ phản ứng của Ukraine được đánh giá rất cao. Nhật báo Anh The Guardian mô tả Diia là một ứng dụng dùng để nộp thuế và cũng để báo cáo về binh sĩ Nga, còn The Economist viết rằng những chatbot như vậy đã biến dân thường Ukraine thành một "lực lượng kháng chiến số".

Nhưng có những vấn đề mà lời khen như vậy không thể làm biến mất. Một báo cáo nhận định rằng Ukraine, thông qua kết nối số, đã làm mờ ranh giới từng tồn tại giữa đóng góp của chiến binh và người không tham chiến, và viết rằng người dân đã trở thành "đôi mắt số" bao phủ toàn bộ lãnh thổ, hoạt động như một yếu tố nhân lực bội tăng. Force multiplier là một thuật ngữ quân sự chỉ một thứ làm phóng đại hiệu quả của binh lực hoặc vũ khí lên nhiều lần mà không cần tăng số lượng của chúng.

"Làm mờ ranh giới" được dùng như một lời khen, nhưng đó là một cụm từ nặng. Luật chiến tranh từ lâu đã phân biệt người mặc quân phục với người không mặc quân phục, và đặt nhóm sau dưới sự bảo vệ. Sự bảo vệ ấy dựa trên tiền đề rằng người không tham chiến không trực tiếp tham gia vào hành động thù địch. Một công dân chụp ảnh vị trí địch bằng điện thoại thông minh rồi đưa chúng lên bản đồ của quân đội thì đứng ở phía nào của tiền đề ấy? Câu hỏi không dừng lại ở Ukraine; nó trở thành câu hỏi của mọi công dân ở mọi quốc gia đang cầm điện thoại thông minh. Sự va chạm giữa huy động tình nguyện trên không gian mạng và luật quốc tế không phải là điều có thể trả lời ngay lúc này, vì vậy câu hỏi vẫn để mở thay vì khép lại.

Có những điều chúng ta không thể xác nhận. Đối với những công dân ở lại trong vùng bị chiếm đóng, việc báo cáo vị trí địch đi kèm nguy hiểm. Nếu bị phát hiện, họ có thể mất mạng, và kênh báo cáo càng rộng thì càng nhiều người phải gánh rủi ro ấy. Không có tài liệu độc lập nào trong số tư liệu được xem xét ở đây cho thấy chính phủ Ukraine đã làm gì để bảo vệ người cung cấp tin, hoặc liệu công dân có bị hại vì các báo cáo của họ hay không. Vì không có nền tảng chứng cứ, vấn đề này được để mở thay vì khép lại quá sớm; ghi rõ rằng chỗ ấy còn trống thì trung thực hơn là tự lấp chỗ trống đó.

Vị trí đặt kênh báo cáo cũng đáng được xem xét. eVorog không nằm trong một ứng dụng do nhà nước xây dựng, mà chạy trên Telegram, một ứng dụng nhắn tin tư nhân. Một báo cáo mô tả chatbot này là một dự án của nhà nước, được xây dựng để ghi nhận chuyển động của quân Nga theo thời gian thực và lưu lại chúng như tài liệu. Nếu đúng như vậy, nền móng của kênh này là máy chủ của một công ty mà chính phủ Ukraine không sở hữu. Không tài liệu nào trong khối tư liệu được thu thập ở đây cho thấy Ukraine đã thỏa thuận gì với Telegram, máy chủ đặt ở đâu, hoặc ai có thể nhìn vào bên trong chúng. Việc nhà nước yêu cầu công dân gửi vị trí quân địch cho mình, trong khi bản thân đường dẫn ấy không nằm trong tay nhà nước, là điều đáng ghi nhận, tách riêng khỏi kết quả mà nó tạo ra.

Thông tin gửi vào sẽ đến DELTA. Các tài liệu mô tả DELTA là một nền tảng chạy trên cloud. Nó xếp thông tin từ drone, vệ tinh, trinh sát và dân thường lên một bản đồ duy nhất, rồi cung cấp cho chỉ huy bức tranh theo thời gian thực. Xếp nhiều lớp là một cách lọc thông tin. Khi nhiều con mắt khác nhau cùng chỉ vào một mục tiêu, độ tin cậy tăng lên; khi chỉ có một con mắt chỉ vào đó, nghi ngờ vẫn còn. Dù vậy, việc xếp lớp không hoàn tất khâu kiểm chứng. Nhiều con mắt có thể cùng chia sẻ một ảo giác, và trên một mặt trận gấp gáp có thể không có thời gian chờ những con mắt khác xuất hiện. Cụm từ "on the cloud" cũng đi kèm một điều kiện. Bản đồ có thể sống động, nhưng một sở chỉ huy bị cắt đường truyền thì không thể mở nó.

Lời khen từ bên ngoài phải được đọc đúng với bản chất của nó. Những câu trong The Guardian và The Economist là ấn tượng từ bên ngoài, không phải các cuộc kiểm toán cân đo mức độ chính xác của hệ thống này. Báo chí ghi lại điều nổi bật, và điều nổi bật đôi khi trùng với kết quả, đôi khi lại tách khỏi kết quả.

Thời gian cũng gắn với các con số. Tổng số 433,000 là con số từ cuối năm 2022. Chúng tôi không xác lập được một thống kê nào muộn hơn cho biết kênh này sau đó có tiếp tục chạy ở cùng quy mô hay không, số báo cáo tăng hay giảm, hoặc người dân có mệt mỏi rồi buông tay hay không. Thứ chúng ta có là một bức ảnh duy nhất chụp ở đoạn cuối năm đầu tiên của cuộc chiến, và sau đó không có đoạn phim nào tiếp nối.

3. Hỗ trợ người tị nạn và khôi phục thiệt hại: Hai mặt của Diia trong thời chiến

Khi chiến tranh bắt đầu, hàng triệu người rời khỏi nơi họ từng sống. Tính đến cuối năm 2023, khoảng 14 triệu người Ukraine đã rời khỏi nhà của mình.

Những người chạy trốn trong vội vã đôi khi không kịp gom theo căn cước và các giấy tờ khác. Những người bỏ lại hộ chiếu giấy và thẻ căn cước, những người mất cả ngăn kéo giấy tờ khi tòa nhà sụp xuống, đã xếp hàng ở biên giới, nhà ga và nơi trú ẩn. Một nhà nước không thể xác nhận họ là ai thì không thể làm gì cho họ. Tiền hỗ trợ, nơi trú ẩn, việc đi qua các trạm kiểm soát, tất cả đều bắt đầu từ xác nhận danh tính. Thêm vào đó, vì chính phủ đã tự tay cắt quyền truy cập vào các sổ đăng ký quốc gia ngay sau cuộc xâm lược, trong một thời gian, ngay cả việc mở giấy tờ điện tử trong Diia cũng khó khăn. Đó là khoảng trống do một biện pháp phòng vệ tạo ra.

Đầu tháng 3 năm 2022, e-Document (єДокумент) được thêm vào Diia. Đây là một giấy tờ điện tử cho phép những người không có hộ chiếu giấy chứng minh danh tính tạm thời, và giấy tờ này chứa thông tin hộ chiếu cùng mã số người nộp thuế. Với một giấy tờ duy nhất này, một người có thể đi qua trạm kiểm soát, đăng ký tại nơi trú ẩn và nộp đơn xin hỗ trợ. Điều mà nhà nước trao lại cho công dân qua giấy tờ này không hẳn là một tờ giấy, mà là một danh tính.

Việc khắc phục thiệt hại được xử lý qua e-Recovery (єВідновлення). Đây là kênh để những công dân có nhà bị phá hủy do pháo kích tải ảnh và thông tin thiệt hại lên qua ứng dụng để yêu cầu bồi thường. Theo số liệu tổng hợp của chính phủ Ukraina, hơn 108.000 công dân đã nhận tổng cộng 10,6 tỷ hryvnia để sửa chữa nhà cửa, và khoảng 23.000 người nhận phiếu nhà ở kỹ thuật số để mua nhà mới, với tổng giá trị 33 tỷ hryvnia. Những con số này là số liệu của chính phủ được một báo cáo công bố vào tháng 11 năm 2025 dẫn lại.

Khi đọc các con số này, cần giữ đồng thời hai điều trong đầu. Những khoản tiền này không phải là số liệu của riêng tháng 2 năm 2022, mà là tổng lũy kế hình thành trong những năm sau đó. Bối cảnh là năm 2022, nhưng để thấy kênh được mở khi ấy sau đó đã chuyên chở những gì, không thể không đưa các con số về sau vào. Và cơ quan lập ra bảng tổng hợp ấy chính là chính phủ đã chi tiền. Trong phần tài liệu được xem xét ở đây, không có tài liệu kiểm toán bên ngoài nào xác nhận khoản bồi thường có thật sự đến tay nạn nhân hay không, bao nhiêu người bị loại trong khâu xét duyệt và vì sao, hoặc bao nhiêu yêu cầu gian lận đã bị lọc ra. Quy mô số tiền đã giải ngân và tính công bằng của hệ thống là hai câu hỏi khác nhau, và với câu hỏi thứ hai thì hiện chưa có nền tảng để trả lời.

Các dịch vụ hành chính vẫn tiếp tục trong chiến tranh. Một báo cáo thống kê rằng 63 phần trăm công dân Ukraina dùng dịch vụ điện tử của nhà nước, và viết rằng từ 130 đến 150 dịch vụ công kỹ thuật số được duy trì không gián đoạn trong thời chiến.

Trong chiến tranh, Diia vừa trở thành phương tiện hỗ trợ đời sống, vừa là kênh nơi quyền lực nhà nước tập trung lại.

Một khuôn mặt là sinh tồn. Nó trả lại căn cước cho những người đã mất thẻ ID, mở đường để tiền đến được với những người mất nhà, và giữ cho bộ máy hành chính tiếp tục vận hành ở những thành phố nơi các tòa nhà chính quyền đã sụp đổ. Khi Nga ném bom các văn phòng để tạo hỗn loạn, Ukraine đã đưa các văn phòng ấy vào trong một ứng dụng.

Khuôn mặt kia là sự tập trung quyền lực. Cùng một ứng dụng vừa là thẻ căn cước, vừa là quầy phúc lợi, vừa là mẫu yêu cầu bồi thường thiệt hại tài sản. Thông tin về một người duy nhất tập hợp dưới một hệ thống xác thực duy nhất, và nguồn tiện lợi cùng nguồn nguy hiểm đi qua cùng một thứ. Lời giải thích rằng kiến trúc của Diia không lưu dữ liệu cá nhân trong ứng dụng có nghĩa là không có gì để lấy nếu đột nhập vào đó. Nếu đọc điều này thành nghĩa nhà nước không thể nhận diện công dân của mình thì sai. Nhà nước luôn có thể nhận diện họ; đó chính là định nghĩa của ID điện tử.

Vì vậy, điều quan trọng là ai kiểm soát công nghệ này và theo thủ tục nào. Ai được tiếp cận dữ liệu này, liệu có còn lại hồ sơ về lần tiếp cận hay không, và nếu có thì ai xem hồ sơ ấy; các ngoại lệ trong thời chiến được cho phép đến đâu và khi nào những ngoại lệ ấy chấm dứt. Một cánh cửa mở ra trong chiến tranh không tự đóng lại khi chiến tranh kết thúc. Phải có người đóng nó, phải có những tiếng nói đòi đóng nó, và để những đòi hỏi ấy có sức nặng thì phải còn lại một

khoảng mở để nêu chúng lên.

Hồ sơ công khai không chứa đủ trải nghiệm của chính công dân. Những tài liệu độc lập cho thấy xã hội dân sự Ukraine hoặc các tổ chức nhân quyền đã phản đối điều gì về Diia và hoạt động giám sát trong quản trị thời chiến, và chính phủ đã trả lời ra sao, vắng mặt một cách rõ rệt trong khối tư liệu được tập hợp ở đây. Lời kể của chính phủ thì có; nguyên văn của lời phê phán thì không. Khi nền móng chỉ nằm ở một phía, cân bằng không phải là thứ có thể tự tạo ra, mà là điều phải thừa nhận là còn thiếu, và khoảng trống này vẫn chưa được lấp đầy.

Còn một nhận định cần ghi lại về tháng 2 năm 2022. Chính phủ điện tử của Ukraine không chứng minh được năng lực của mình bằng cách đối mặt với chiến tranh; mục đích của nó đã thay đổi. Một công cụ được xây dựng để xóa bỏ cảnh xếp hàng đã đứng cạnh một đường dẫn dùng để tìm mục tiêu. Một hệ thống xác thực được xây dựng để thu thuế trở thành khung quản trị thời chiến. Một quầy từng tiếp nhận hồ sơ phúc lợi nay tiếp nhận ảnh chụp những ngôi nhà đổ nát. Sự chuyển đổi này diễn ra nhanh, và nhiều tài liệu ghi nhận rằng nó đã vận hành được. Chuyển đổi nhanh thường bỏ qua cân nhắc. Những cân nhắc bị bỏ qua không biến mất; chúng chất lại phía sau, và thứ đã chất lại một ngày nào đó sẽ quay trở lại dưới dạng hóa đơn phải trả.

Các kênh được mở trong thời chiến không mọc lên từ nền đất trống. Khi ứng dụng và cổng Diia xuất hiện vào năm 2020, một hệ thống chi trả cứu trợ COVID-19 cho công dân cũng được mở cùng lúc. Trước tiên, Ukraine đã trải qua kinh nghiệm một nhà nước gửi tiền bằng ứng dụng cho những người bị tai họa trong một trận dịch. e-Recovery năm 2022 không hẳn là mở một con đường mới, mà là đặt một gánh nặng khác lên con đường đã được mở sẵn.

Diia cũng được dùng để gửi các khoản hỗ trợ cho công dân. Trong Diia có chức năng để người phải rời nơi ở đăng ký nơi cư trú mới và nộp đơn xin hỗ trợ hằng tháng của chính phủ, và chức năng mua trái phiếu chiến tranh, tức công cụ huy động tiền cho chi phí chiến tranh, cũng được gắn thêm. Một bên là tiền của nhà nước đi ra đến công dân; bên kia là tiền của công dân đi vào nhà nước. Một màn hình duy nhất trở thành chiếc ví nhìn về hai hướng.

Con số 63 phần trăm người dân dùng dịch vụ điện tử của nhà nước phải được đọc theo chiều ngược lại. Nó có nghĩa là vẫn còn những người không dùng các dịch vụ đó. Có người không có điện thoại thông minh, có người sống gần tiền tuyến và đường liên lạc bị cắt, có người quá già để dùng một ứng dụng. Trong các tài liệu được xem xét ở đây, không có tài liệu nào cho thấy những người này chứng minh danh tính ở đâu trong thời chiến, hoặc họ yêu cầu bồi thường qua kênh nào. Ở một quốc gia đã đưa bộ máy hành chính vào trong một ứng dụng, người đứng ngoài ứng dụng sẽ đi đâu? Chúng ta không có nền tảng để trả lời câu hỏi đó, và viết rằng nền tảng ấy vắng mặt thì chính xác hơn là giả vờ như nó có ở đó.

Hình thức giám sát tồn tại trên giấy tờ. Bộ Chuyển đổi Số quản lý Trembita và Diia, đồng thời giữ vai trò điều phối trong các dự án số của chính phủ, còn Ủy ban Chuyển đổi Số của quốc hội hỗ trợ công việc này. Nhưng trong phần tài liệu được thu thập ở đây, không có hồ sơ nào cho

thấy ủy ban đó đã thảo luận những gì trong thời chiến, đã đưa ra nhận định gì về việc cắt quyền truy cập vào các cơ sở đăng ký quốc gia hoặc về các ngoại lệ thời chiến, hay đã quyết định khi nào các ngoại lệ ấy sẽ được rút lại. Việc có một cơ quan giám sát tồn tại và việc hoạt động giám sát đã thật sự diễn ra là hai mệnh đề khác nhau. Mệnh đề thứ nhất đã được xác nhận; còn với mệnh đề thứ hai, hồ sơ công khai dừng lại ở đây.

Chương 3. IT Army, lực lượng tình nguyện trong không gian mạng

Ngày 26 tháng 2 năm 2022, một thông điệp ngắn xuất hiện trên kênh Telegram chính thức của Mykhailo Fedorov, Bộ trưởng Chuyển đổi Số của Ukraine. Đó là lời kêu gọi bất kỳ ai biết xử lý công nghệ số, không phân biệt quốc tịch, hãy đứng về phía Ukraine. Khi ấy là ngày thứ ba của cuộc xâm lược toàn diện, và phản ứng đến rất nhanh. Không lâu sau, kênh này đã tăng lên khoảng 150,000 người đăng ký.

Tổ chức này được gọi là IT Army of Ukraine. Chữ army được gắn vào tên gọi, nhưng không có doanh trại và không có phù hiệu. Thông báo tuyển người đến từ tài khoản mạng xã hội của một bộ trưởng phụ trách kỹ thuật số, còn người đăng ký không phải khám sức khỏe và cũng không tuyên thệ. Bạn đăng ký theo dõi kênh, hướng máy tính của mình vào mục tiêu trên màn hình, và như vậy là nhập ngũ. Không cần nhận vũ khí, không cần được phân về một đơn vị. Chỉ cần một thiết bị kết nối internet và quyết định làm theo một danh sách.

Các bài viết và bài giảng về tổ chức này thường nói rằng số người tham gia là bốn trăm nghìn. Con số có thể xác nhận trong tài liệu nền là khoảng 150,000 người đăng ký kênh Telegram. Nguồn gốc trực tiếp của con số bốn trăm nghìn không tìm thấy ở bất kỳ đâu trong hồ sơ công khai, nên ở đây chỉ dùng phạm vi đã được xác nhận.

Số người đăng ký và số người thật sự tham gia các cuộc tấn công ngay từ đầu đã là hai đại lượng khác nhau. Một người đăng ký kênh nhưng chưa từng chạy công cụ lần nào vẫn được tính là người đăng ký. Ngược lại, một người chưa từng đăng ký nhưng tải xuống và chạy các chương trình được phân phối lại không nằm trong số người đăng ký. Quân số của tổ chức này thay đổi rất lớn tùy theo cách đếm, và quy mô của IT Army đến nay vẫn chưa được biết rõ.

1. Một cuộc huy động vượt ra ngoài nhà nước, bắt đầu trên Telegram

Người đầu tiên đề xuất IT Army là một doanh nhân ngoài chính phủ. Hai báo cáo phân tích ghi nhận rằng điểm khởi đầu là đề xuất của doanh nhân IT người Ukraine Yegor Aushev gửi Bộ trưởng Fedorov về việc lập một nhóm tình nguyện an ninh mạng. Một báo cáo do New Strategy Center của Romania công bố vào tháng 6 năm 2024, báo cáo còn lại là bản nhìn lại một năm chiến tranh do CERT-EU, đội ứng cứu khẩn cấp máy tính của các định chế European Union, công bố vào tháng 2 năm 2023.

Ý tưởng đến từ khu vực tư nhân, và vị bộ trưởng là người đưa đề xuất ấy lên một kênh mà cả thế giới có thể nhìn thấy rồi tập hợp mọi người quanh nó. Việc Fedorov làm gần với khuếch đại hơn là sáng lập. Ông cho một đề xuất tư nhân mượn chiếc loa phóng thanh của nhà nước. Người mở kênh cho lời kêu gọi và người chỉ đạo mọi việc do những người hưởng ứng thực hiện không phải là cùng một người, và sự phân biệt này sẽ còn được dùng lại khi cân nhắc công và

lỗi của ông.

Các nguồn tư liệu thậm chí còn không thống nhất về ngày thành lập. Một số đặt thời điểm khởi đầu của IT Army vào ngày 25 tháng 2 năm 2022, số khác vào ngày 26 tháng 2. Thay vì chọn một ngày, cả hai ngày đều được giữ lại. Chênh lệch một ngày có thể trông nhỏ, nhưng trong cuộc tranh luận theo luật quốc tế về thời điểm nhà nước bắt đầu dính líu đến tổ chức này, ngày đó trở thành một nền tảng. Sự chao đảo về ngày tháng trong hồ sơ chiến tranh phản ánh hoàn cảnh tổ chức này ra đời từ một bài đăng mạng xã hội khẩn cấp.

Muốn thấy những người được tập hợp ấy thật sự đã làm gì, phải nhìn vào công cụ. Công cụ chính của IT Army là tấn công DDoS (distributed denial of service, tấn công từ chối dịch vụ phân tán). Thuật ngữ nghe có vẻ khó, nhưng nguyên lý thì không. Khi rất nhiều máy tính cùng lúc đổ yêu cầu kết nối vào một website duy nhất, máy chủ vượt quá lưu lượng mà nó có thể xử lý và ngừng hoạt động. Nó giống như một lối cửa hẹp bị chen kín cùng một lúc, khiến những người thật sự có việc cần vào đó không thể ra vào được.

Phương pháp này không làm được gì nếu chỉ có một máy tính. Hàng chục nghìn máy phải cùng chuyển động thì mới thành một bức tường, và số lượng tình nguyện viên tự nó chính là hỏa lực. Vì vậy, với IT Army, hạ thấp ngưỡng tham gia trực tiếp dẫn đến việc tăng sức mạnh của tổ chức.

Các tình nguyện viên đưa băng thông liên lạc từ chính máy tính của mình vào để tạo thành một botnet khổng lồ. Botnet có nghĩa là một đàn máy tính cùng chuyển động theo một mệnh lệnh duy nhất. Những công cụ tự động hóa cần cho việc này do chính các hacker xây dựng và phân phối. Bohdan Ivashko (handle: Arriven), một kỹ sư gốc Ukraine làm việc tại công ty an ninh Mỹ Cyberhaven, đã phát hành một chương trình tên là db1000n trên GitHub. GitHub là một kho lưu trữ công khai, nơi các nhà phát triển tải mã chương trình lên để bất kỳ ai cũng có thể tải xuống. Một công cụ tên là disBalancer, dùng mạng Web 3.0, xuất hiện; IT ARMY Kit, gói nhiều công cụ thành một, cũng được phân phối. Chúng có hình thức mà ngay cả người không biết gì về lập trình cũng có thể tải xuống, bấm nút chạy và gia nhập hàng ngũ. Đây là một cuộc chiến trong đó cá nhân tự chế tạo vũ khí, cá nhân tự phân phối chúng, rồi cá nhân tải xuống và sử dụng chúng.

Tính chất của cuộc huy động này, đúng như tên gọi, đã vượt ra ngoài nhà nước. Người tham gia không nhất thiết phải là công dân Ukraine; họ sống ở đâu trên thế giới cũng được, chỉ cần có internet. Những người xây dựng công cụ, và những nơi đặt các công cụ ấy, là các cá nhân và các nền tảng tư nhân như GitHub. Chính sân khấu nơi tổ chức vận hành là Telegram, một ứng dụng nhắn tin tư nhân. Nhà nước chỉ là tiếng nói công bố mục tiêu, chứ không phải chủ sở hữu của tổ chức.

Khi những người có quốc tịch, nơi cư trú và quan hệ tổ chức khác nhau cùng tụ lại, điểm đặt trách nhiệm trở nên mờ đi. Câu hỏi là nhà nước phải gánh bao nhiêu trách nhiệm đối với một

lực lượng được tổ chức vượt ra ngoài nhà nước, có người tham gia vượt ra ngoài nhà nước, và vận hành bằng những công cụ cũng vượt ra ngoài nhà nước.

Bên trong tổ chức ấy không phải chỗ nào cũng phẳng. Báo cáo của New Strategy Center phân tích IT Army như một cấu trúc pha trộn giữa mạng lưới tình nguyện ngang hàng và chuỗi chỉ huy theo chiều dọc. Ở tầng trên cùng là 25 đến 30 chuyên gia IT được rút từ các cơ quan tình báo và bộ ngành của Ukraine, và báo cáo gọi họ là các Generals. Họ chỉ đạo một nhóm hacker lành nghề, có năng lực xâm nhập thật sự, được gọi là Colonels, trên một nền tảng bảo mật riêng. Những tình nguyện viên thông thường nhận danh sách mục tiêu được đăng công khai trên Telegram là lớp ngoài của cấu trúc này.

Điều đó có nghĩa là từ bên ngoài, thứ nhìn thấy được là một kênh Telegram duy nhất, nhưng phía sau nó còn có hai lớp vô hình nữa. Một tình nguyện viên ở lớp ngoài có thể đã bấm nút chạy mà không biết mình đang thực hiện kế hoạch của ai.

Cấu trúc này có ý nghĩa khi cân nhắc công và lỗi cá nhân của Fedorov. Việc ông đăng trên Telegram và tập hợp được một nhóm người theo dõi khoảng 150.000 là sự thật đã được xác nhận. Nhưng các Generals nhận chỉ đạo gì từ chính phủ, ai đưa ra quyết định cuối cùng về mục tiêu, và vai trò được chia ra sao giữa Ministry of Digital Transformation và các cơ quan tình báo, thì hồ sơ công khai hiện chưa cho phép kết luận. Không thể từ đó suy ra rằng người mở cánh cửa là chỉ huy của mọi việc xảy ra bên trong. Phần của Fedorov rõ ở việc mở cánh cửa; những gì nằm phía sau cánh cửa ấy vẫn còn mờ.

Fedorov có thể nói chuyện với lực lượng lao động kỹ thuật trên toàn thế giới vào ngày thứ ba của cuộc xâm lược vì kênh đó không phải là thứ được vội vàng dựng lên khi chiến tranh bùng nổ. Bộ Chuyển đổi Số của Ukraine được thành lập vào năm 2019. Đây là bộ được giao thực hiện cam kết mà Tổng thống Volodymyr Zelensky đưa ra trong cuộc bầu cử năm 2019, "nhà nước trong một chiếc điện thoại thông minh", và năm 2020 ứng dụng di động quốc gia Diia xuất hiện. Trước cuộc xâm lược, Diia đã thu hút khoảng hai mươi hai triệu người dùng và được cài đặt trên 77 phần trăm điện thoại thông minh của Ukraine. Diia.City, nơi cấp ưu đãi thuế cho các công ty IT, đã có hàng nghìn doanh nghiệp tham gia. Một kênh để nói trực tiếp với công dân và với ngành công nghệ đã vận hành được vài năm.

Bộ Chuyển đổi Số cũng mở một kênh để công dân gửi báo cáo ngay từ giai đoạn đầu của cuộc chiến. Chatbot eVorog, qua đó công dân báo cáo hoạt động di chuyển và vị trí của quân đội Nga kèm ảnh và dữ liệu vị trí, vận hành song song với kênh này. Đến cuối năm 2022, hơn 433.000 công dân đã gửi thông tin quân sự qua chatbot này, và thông tin đó được kiểm chứng rồi đưa vào Delta. Delta là một hệ thống quân sự gom các báo cáo rời rạc và dữ liệu trinh sát lên một màn hình duy nhất để cho thấy thứ gì đang ở đâu. Chatbot được thiết kế để yêu cầu xác minh danh tính qua Diia, nhằm chặn các báo cáo giả do đối phương cài vào.

Hai tổ chức khác nhau về cách tham gia và chuỗi chỉ huy. eVorog chỉ cho phép những người đã được xác minh danh tính qua một ứng dụng nhà nước tham gia, và thông tin gửi vào được lọc qua các hệ thống của quân đội. IT Army thì được tham gia bằng một nút đăng ký Telegram duy nhất, và trong hồ sơ công khai không có chỗ nào ghi lại thủ tục xác minh danh tính người tham gia. Một bên còn lại hồ sơ ai đã gửi gì; bên kia không còn hồ sơ ai đã bấm gì.

Cần giữ sự phân biệt này khi xử lý các con số. 433.000 là con số được ghi nhận là số người cung cấp tin qua eVorog, còn con số có thể xác nhận đối với IT Army là khoảng 150.000 người đăng ký Telegram. Hồ sơ công khai không nối hai con số này với nhau. Con số bốn trăm nghìn xuất phát từ đâu là điểm mà hồ sơ công khai dừng lại.

2. Cuộc tranh luận trong luật quốc tế về mục tiêu, người tham gia và chỉ huy

IT Army trở thành vấn đề trên bàn làm việc của các học giả luật quốc tế vì nó không nằm gọn trong bất kỳ ô nào của bộ quy tắc hiện có. Chiến tranh cũng có luật lệ. Các hệ thống quy tắc được gọi là luật nhân đạo quốc tế (IHL) và luật xung đột vũ trang (LOAC) quy định ai được tham chiến, mục tiêu nào được phép tấn công, và ai phải chịu trách nhiệm. IT Army làm mờ câu trả lời cho cả ba câu hỏi ấy.

Trước hết là câu hỏi mục tiêu nào được phép tấn công.

Nghị định thư bổ sung I của các Công ước Geneva năm 1977 yêu cầu các bên tham chiến chỉ tấn công các mục tiêu quân sự. Một mục tiêu quân sự là đối tượng mà việc phá hủy hoặc vô hiệu hóa nó đem lại một lợi thế quân sự rõ ràng. Đồng thời, phải giữ sự tương xứng giữa lợi thế quân sự đạt được và thiệt hại mà dân thường phải gánh chịu. Khuôn khổ này được áp dụng lại cho không gian mạng trong một báo cáo do Atlantic Council công bố vào tháng 11 năm 2025. Ủy ban Chữ thập đỏ Quốc tế (ICRC) đã đưa ra tám quy tắc mà các hacker dân sự tham gia trong thời chiến phải tuân thủ: không trực tiếp nhắm vào cơ sở dân sự; không dùng phần mềm độc hại lan truyền bừa bãi qua cả mục tiêu quân sự lẫn cơ sở dân sự; không đụng tới cơ sở y tế hoặc nhân đạo; không tấn công hạ tầng thiết yếu cho sự sống còn của dân thường; và các quy tắc tương tự khác.

Khó có thể nói IT Army đã vi phạm tất cả các quy tắc này. Báo cáo ghi nhận rằng họ dè dặt khi nhắm vào lĩnh vực y tế và hỗ trợ xã hội. Điều đó có nghĩa là họ đã cố tránh động đến bệnh viện. Vấn đề nằm ở phần tiếp theo. Các mục tiêu chính được ghi trong cùng báo cáo là các ngân hàng như Sberbank, Gazprombank và VTB; nền tảng video Rutube; Sàn giao dịch Moscow; và cổng Troika, hệ thống xử lý thanh toán tiền vé trên 38 vùng. Đây là những hệ thống mà qua đó công dân Nga trả tiền xe buýt, nhận lương và xem video. Hạ tầng dân sự giữ cho đời sống hằng ngày vận hành đã chiếm một phần lớn trong danh sách mục tiêu.

IT Army nêu mục tiêu là làm giảm nguồn lực kinh tế của Nga, qua đó làm suy yếu năng lực tiến hành chiến tranh của nước này. Nhưng các cuộc tấn công vào dịch vụ dân sự có chuyển thành lợi thế quân sự hay không thì không rõ. Sự bất tiện mà một công dân Nga chịu khi ứng dụng ngân hàng ngừng hoạt động trong vài giờ có phải là một lợi thế quân sự rõ ràng theo nghĩa của luật quốc tế không? Làm sao đo được mối liên hệ nhân quả giữa việc làm rung chuyển một mạng lưới thanh toán và kết quả các trận đánh ở tiền tuyến? Ngay cả trong các viện nghiên cứu chính sách phương Tây, cuộc tranh luận này vẫn chưa ngã ngũ. Khi tiêu chí chọn mục tiêu bị làm mờ, cái giá của sự mập mờ ấy do dân thường ở quốc gia bị nhắm đến gánh chịu.

Tiếp theo là câu hỏi liệu những người tham gia là binh sĩ hay dân thường. Việc họ được đối xử như tù binh chiến tranh khi bị bắt hay bị đưa ra xét xử như tội phạm phụ thuộc vào điều này, nên đây là sự phân biệt gắn với mạng sống và tự do của con người.

Có những điều kiện để trở thành chiến binh theo nghĩa của luật quốc tế. Theo Điều 4(A) của Công ước Geneva thứ ba và các Điều 43, 44 của Nghị định thư bổ sung I, một người phải thuộc lực lượng vũ trang chính quy của một bên tham chiến, hoặc thuộc dân quân hay quân đoàn tình nguyện được tích hợp vào lực lượng đó; phải đặt dưới quyền chỉ huy của một cấp trên; phải mang một dấu hiệu phân biệt có thể nhận ra từ xa; phải mang vũ khí công khai; và phải tuân thủ luật nhân đạo quốc tế trong hoạt động tác chiến. Cũng có một ngoại lệ, levée en masse, dành cho cư dân tự phát cầm vũ khí khi quân đội xâm lược đang áp sát.

IT Army không đáp ứng bất kỳ điều kiện nào trong số đó. Lực lượng này không được sáp nhập vào quân đội chính quy, không có quân phục, và một chiếc máy tính xách tay không thể được gọi là vũ khí mang công khai. Các thành viên của họ rải rác khắp thế giới, nên cũng không thể được xem là một cuộc nổi dậy của cư dân trong lãnh thổ bị chiếm đóng. Vì vậy, về mặt pháp lý, họ là thường dân; dù gây ra thiệt hại thật trong chiến tranh, địa vị của họ lại xếp họ vào nhóm người không gắn với cuộc chiến đó.

Khi thường dân nhúng tay vào chiến tranh, câu hỏi tiếp theo là việc đó có cấu thành tham gia trực tiếp vào chiến sự hay không, tức direct participation in hostilities (DPH). Cả ba điều kiện đều phải được đáp ứng. Hành vi đó phải gây chết người, gây thương tích, gây phá hủy vật chất, hoặc có tác động bất lợi đáng kể đối với hoạt động quân sự của đối phương, tức ngưỡng thiệt hại; phải có mối liên hệ nhân quả trực tiếp giữa hành vi và thiệt hại; và mục đích phải là hỗ trợ một bên tham chiến, đồng thời gây hại cho bên kia.

Nhận định của báo cáo đi theo hướng này. Điều kiện cuối cùng được đáp ứng. Ý định giúp Ukraine của họ là rõ ràng. Nhưng các cuộc tấn công DDoS và việc thay đổi giao diện website không giết ai, không làm ai bị thương, cũng không phá vỡ đồ vật. Thay đổi giao diện nghĩa là thay trang chủ website của người khác bằng thông điệp của chính mình. Vì vậy, điều kiện về ngưỡng thiệt hại không được đáp ứng.

Khi áp dụng luật, địa vị của họ trở thành một địa vị rất khó được bảo vệ. Các tình nguyện viên của IT Army không đáp ứng yêu cầu để được coi là chiến binh, nên không được hưởng sự bảo vệ dành cho tù binh chiến tranh. Đồng thời, họ cũng không đáp ứng yêu cầu về tham gia trực tiếp, nên không được công nhận là đang thực hiện hành vi chiến tranh hợp pháp. Nếu bị Nga bắt, họ có thể bị trừng phạt như tội phạm tin tặc theo luật hình sự Nga. Hàng chục nghìn người đã bước vào một khoảng trống của pháp luật, không có sự bảo vệ, cũng không có địa vị pháp lý. Ngưỡng tham gia càng thấp, bản chất của rủi ro càng có thể trở nên khó thấy, ngay cả đối với chính những người tham gia.

Trách nhiệm của nhà nước cũng phải được xem xét.

Có một văn kiện đặt ra các chuẩn mực pháp lý cho hoạt động mạng, đó là Tallinn Manual 2.0. Đây là bản bình luận do một nhóm chuyên gia có liên hệ với NATO biên soạn. Quy tắc 15 và 17 nêu rằng khi một chủ thể phi nhà nước tiến hành hoạt động theo chỉ thị, sự chỉ đạo hoặc sự kiểm soát của một nhà nước, hành vi đó được quy cho nhà nước ấy. Vấn đề nằm ở chỗ phải hiểu mức độ kiểm soát nghiêm ngặt đến đâu, và tại đây hai nguyên tắc va chạm với nhau.

Một bên là học thuyết kiểm soát hữu hiệu (ECD). Xuất phát từ vụ Nicaragua của Tòa án Công lý Quốc tế, chuẩn mực này chỉ công nhận trách nhiệm khi chứng minh được một cách chắc chắn rằng nhà nước đã kiểm soát trực tiếp và toàn diện tổ chức đó. Ngưỡng chứng minh rất cao. Bên kia là học thuyết kiểm soát tổng thể (OCD). Học thuyết này xuất hiện từ vụ Tadić tại Tòa án Hình sự Quốc tế về Nam Tư cũ (ICTY), và cho rằng một nhà nước có thể bị quy trách nhiệm ngay cả khi nhà nước đó chỉ đóng vai trò tổ chức, điều phối và hỗ trợ tổ chức ấy. Ngưỡng chứng minh thấp. Với cùng một tập hợp sự kiện, việc dùng thước đo nào sẽ đảo ngược câu trả lời về việc có hay không có trách nhiệm của nhà nước.

Theo chuẩn ECD nghiêm ngặt, chính phủ Ukraine vẫn còn khoảng trống để thoát khỏi trách nhiệm. Việc chứng minh rằng chính phủ đã trực tiếp ra lệnh cho từng cuộc tấn công riêng lẻ không dễ. Theo chuẩn OCD rộng hơn, tình hình lại khác. Chừng nào người tham gia còn được tập hợp qua kênh của một bộ trưởng và còn có một Telegram nơi các danh sách mục tiêu được trao đổi, thì rất khó phủ nhận dấu vết của sự điều phối và hỗ trợ.

Báo cáo đưa ra một bảng trình bày mức độ trách nhiệm của nhà nước qua mười cấp. Cấp 1 là giai đoạn một nhà nước cấm và ngăn chặn các cuộc tấn công do bên thứ ba thực hiện, còn cấp 10 là giai đoạn lực lượng chính quy của một nhà nước và các lực lượng ủy nhiệm bên thứ ba được hợp nhất hoàn toàn. Trên thang đo này, vị trí của chính phủ Ukraine vào đầu cuộc chiến hoặc là phối hợp của nhà nước (cấp 6), tức đề xuất các chi tiết tác chiến, hoặc là khuyến khích của nhà nước (cấp 4), tức thúc đẩy các cuộc tấn công như một vấn đề chính sách. Đó là vai trò đã tham gia nhưng không sở hữu.

Vị trí pháp lý này có thể thay đổi. Quốc hội Ukraine và Ministry of Digital Transformation đã chuẩn bị một dự thảo luật an ninh mạng, theo đó các đơn vị hacker tình nguyện sẽ được hợp

pháp hóa như một lực lượng dự bị mạng của lực lượng vũ trang chính quy và được sáp nhập vào đó. Nếu luật này được thông qua, IT Army sẽ đi vào tổ chức của nhà nước theo cách đơn vị phòng thủ mạng của Estonian Defence League đã làm, và trách nhiệm của nhà nước Ukraine sẽ tăng lên bậc cao nhất, hợp nhất với nhà nước (cấp 10). Điều đó có nghĩa là nhà nước sẽ gánh đầy đủ trách nhiệm pháp lý quốc tế và nghĩa vụ bồi thường phát sinh từ hoạt động hacking do các tình nguyện viên thực hiện. Dự luật về lực lượng dự bị mạng vẫn là một kế hoạch ở giai đoạn dự thảo, và hồ sơ công khai chỉ dừng lại ở đây về việc nó có được thông qua và thi hành hay không.

Đưa họ vào khuôn khổ pháp luật thì các tình nguyện viên có được sự bảo vệ, còn nhà nước nhận lấy trách nhiệm. Để họ ở bên ngoài thì nhà nước tránh được trách nhiệm, còn các tình nguyện viên mất đi sự bảo vệ. Khi Fedorov đăng một thông điệp duy nhất lên Telegram, vấn đề này, dù đi theo hướng nào cũng phải trả giá, đã được mở ra cùng lúc.

Cần nói rõ các thước đo được dùng trong cuộc tranh luận này thật ra là loại tài liệu gì. Tallinn Manual 2.0 không phải là một điều ước được các nhà nước ký kết, mà là một bản bình luận do một nhóm chuyên gia có liên hệ với NATO viết ra. Bảng trình bày trách nhiệm của nhà nước qua mười cấp cũng không phải là luật, mà là một thang đo do Romania's New Strategy Center tạo ra để phân tích. Tám quy tắc của ICRC cũng vậy, không phải là các điều khoản áp đặt hình phạt khi bị vi phạm, mà là các khuyến nghị kêu gọi tuân thủ. Có nhiều tài liệu nói về quy tắc, nhưng trong hồ sơ công khai chưa có phán quyết nào của một tòa án quốc tế áp dụng những quy tắc đó cho IT Army và đưa ra phán xử. Có nhiều thước đo, còn phòng xử án thì vẫn chưa mở cửa.

Tin tặc không phải là những người duy nhất đứng trong vùng xám. Một báo cáo về hệ thống an ninh mạng thời chiến của Ukraine ghi nhận rằng kiểu tham gia của công dân như vậy đã làm mờ ranh giới giữa đóng góp của chiến binh và người không tham chiến. 433.000 công dân đã chụp ảnh hoạt động di chuyển của quân Nga và tải chúng lên một chatbot cũng đứng trước cùng câu hỏi ấy. Giữa người chạy công cụ DDoS và người tải lên một bức ảnh, ai gần với chiến tranh hơn? Những ô phân loại cũ của luật quốc tế không có câu trả lời.

Mô hình mà dự luật sáp nhập tự đem ra so sánh cũng đáng được kiểm chứng. Mô hình được báo cáo viện dẫn là đơn vị phòng thủ mạng của Estonian Defence League. Đó là cách đưa tình nguyện viên vào bên trong tổ chức của nhà nước và đặt họ dưới một chuỗi chỉ huy cùng kỷ luật. Khi đã ở bên trong, tình nguyện viên có địa vị và sự bảo vệ, còn nhà nước cùng họ gánh nghĩa vụ bồi thường cho những việc họ đã làm. Khoản bồi thường ấy sẽ được trả cho ai, theo thủ tục nào, và những người đã dùng Sberbank hay cổng Troika có thể yêu cầu gì, thì hồ sơ công khai không ghi rõ.

Các bên liên quan cũng không dừng lại ở chính phủ và tình nguyện viên. GitHub, nơi các công cụ được đặt, và Telegram, nơi tổ chức vận hành, đều là dịch vụ của các công ty tư nhân. Những công ty này đã xử lý những gì xảy ra trên nền tảng của họ ra sao, liệu họ có thể gỡ các công cụ

xuống hoặc chặn kênh hay không, hồ sơ công khai không cho biết. Ở nơi các quy tắc chiến tranh được tranh luận, chính những bên sở hữu sân khấu lại vắng mặt.

3. Mạng lưới tình nguyện đã đạt được gì và khoảng trống nơi lẽ ra phải có kiểm soát

Đòn tấn công tiêu biểu được ghi trong báo cáo của New Strategy Center là vụ tấn công Rutube đúng dịp Ngày Chiến thắng của Nga, ngày 9 tháng 5 năm 2022. Báo cáo nói rằng mật khẩu quản trị viên đã bị thay đổi và dữ liệu ở quy mô một petabyte đã bị xóa. Một petabyte lớn gấp khoảng một triệu lần một gigabyte. Bên cạnh đó còn ghi nhận các trường hợp Moscow Exchange, Tinkoff Bank và Troika, cổng thanh toán giao thông công cộng cho 38 vùng, bị làm cho tê liệt.

Không có một xu nào từ ngân sách quân sự thường xuyên, không có một cuộc điều quân nào, họ đã làm rung chuyển hạ tầng sinh hoạt hằng ngày của đối phương trong nhiều ngày liền. Chỉ bằng những chiếc máy tính xách tay rẻ tiền và thời gian của các tình nguyện viên, họ tạo ra một biến động có thể sánh với một chiến dịch chính quy tốn kém.

Vấn đề tiếp theo là không ai đo lường quy mô của thành quả đó. Tác động của một cuộc tấn công DDoS thường chỉ là tạm thời. Máy chủ ngừng hoạt động trong vài giờ, nhiều nhất là vài ngày, rồi hoạt động trở lại. Chính việc không gây phá hủy vật lý là yếu tố khiến địa vị pháp lý của họ trở nên mơ hồ. Trong hồ sơ công khai, không thể xác nhận có tài liệu độc lập nào đo lường những cuộc tấn công này thực sự đã làm giảm năng lực tiến hành chiến tranh của Nga đến mức nào; chỉ có các thông báo từ phía Ukraine và các bản tự thuật của người tham gia. Nguyên tắc không đặt thông báo ngang hàng với kiểm chứng độc lập cũng được áp dụng ở đây như ở mọi nơi khác.

Sự kiểm soát cũng trống rỗng. Theo thời gian, IT Army dần tách khỏi nhà nước. Theo báo cáo, sự hỗ trợ của chính phủ thu hẹp xuống mức hỗ trợ phi tác chiến, và tổ chức này vận hành theo mô hình phân tán, tự gây quỹ thông qua crowdfunding. Crowdfunding là phương thức gom nhiều khoản đóng góp nhỏ qua internet. Một tổ chức do nhà nước gọi ra đời đã trượt khỏi tay nhà nước; một tiếng loa phóng thanh là đủ để gọi nó đến, nhưng để xoay nó lại thì không có chiếc loa phóng thanh nào như vậy.

Hoàn cảnh có quy tắc nhưng không có bàn tay nào thực thi ngay lập tức hiện ra như một vấn đề thực tế. ICRC đã đưa ra tám quy tắc dành cho các hacker dân sự, nhưng không có cách nào buộc hàng chục nghìn người chỉ liên kết lỏng lẻo qua một kênh Telegram phải tuân theo những quy tắc ấy. Nếu ai đó đánh vào mạng máy tính của một bệnh viện, ai sẽ ngăn họ lại? Ai sẽ trừng phạt họ? Một đội quân không có người chỉ huy thì cũng không có quân luật. Điểm mạnh của tổ chức này, rằng ai cũng có thể tham gia, nguyên vẹn trở thành điểm yếu của nó. Nói rằng ai cũng có thể tham gia đi liền với nói rằng không ai chịu trách nhiệm, và sự mở cửa đã làm tổ

chức lớn lên cũng chính là sự mở cửa khiến nó không thể bị kiểm soát.

Những con số và sự kiện cũng mang theo các câu hỏi nằm ngoài hồ sơ công khai. Quy mô bốn trăm nghìn người thường được trích dẫn rộng rãi là điểm mà hồ sơ công khai dừng lại. Điều có thể xác nhận chỉ là một con số duy nhất: khoảng 150.000 người đăng ký Telegram. Ngày thành lập bị chia giữa ngày 25 và 26 tháng 2. Quan hệ chỉ huy giữa 25 đến 30 Generals trong ban lãnh đạo với chính phủ cũng là vấn đề vẫn còn quá sớm để kết luận. Khó có thể hy vọng hồ sơ của một tổ chức được tạo ra giữa chiến tranh sẽ còn nguyên vẹn. Nhưng ghi lại sự thật rằng hồ sơ vắng mặt là việc có thể làm, và để khoảng trống đúng là khoảng trống thay vì giả vờ đã lấp đầy nó, đó là cách xử lý tổ chức này một cách trung thực.

Các báo cáo vẫn tiếp tục xuất hiện ngay cả sau khi những sự kiện ấy đã qua. CERT-EU đã tóm tắt năm đầu tiên của các chiến dịch mạng trong cuộc chiến vào tháng 2 năm 2023. New Strategy Center của Romania công bố một báo cáo về mặt trận số phía đông vào tháng 6 năm 2024. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) xuất bản một tài liệu về sự phát triển của năng lực phòng thủ mạng của Ukraine vào tháng 3 năm 2026, và Australian Army Research Centre phát hành OP 35, một bài nghiên cứu về IT Army, vào ngày 22 tháng 4 năm 2026. Việc các viện nghiên cứu quân sự ở nhiều nước vẫn bám sát cùng một tổ chức trong nhiều năm sau cuộc xâm lược có nghĩa là các kết luận vẫn chưa ngã ngũ.

Điều có thể xác nhận như công lao của ông là tốc độ. Vào ngày thứ ba của cuộc xâm lược, ông mở một kênh chạm tới lực lượng kỹ thuật trên toàn thế giới và kéo được phản ứng ở quy mô 150.000 người. Nếu bộ quốc phòng tổ chức một lực lượng tình nguyện theo đúng thủ tục, việc đó sẽ mất nhiều tháng. Người có ý tưởng là doanh nhân tư nhân Aushev, những người xây dựng công cụ là các nhà phát triển như Ivashko, và việc vị bộ trưởng làm là gắn chiếc loa phóng thanh của nhà nước vào dòng chảy ấy.

Điều hiện ra là vai trò mà chiếc loa phóng thanh ấy đã tạo ra. Hàng chục nghìn người được tập hợp qua một kênh nhà nước đã đứng vào một vị trí không có mệnh lệnh của nhà nước, cũng không có sự bảo vệ của nhà nước. Về pháp lý, họ là dân thường; nếu bị bắt, họ trở thành tội phạm; và nếu họ phá luật, không có ai ngăn họ lại. Không có cơ sở để nói rằng trách nhiệm về tình trạng này hoàn toàn thuộc về một mình Fedorov. Nhưng sự thật vẫn còn đó: tình trạng này bắt đầu từ bài đăng Telegram của ông, và ông là người thiết kế một cuộc huy động nhanh, đồng thời là người thiết kế một cuộc huy động không có kiểm soát.

Với một chiếc máy tính và internet, một người có thể tham gia một cuộc chiến từ bên ngoài biên giới của nó. Khi khoảng cách giữa bàn tay cầm smartphone và tiền tuyến biến mất, khoảng cách giữa chiến binh và dân thường cũng biến mất theo. Thứ còn lại trên đường ranh đã bị xóa ấy là một con số người đăng ký khoảng 150.000 và một hồ sơ chưa bao giờ xác định rõ họ tuân theo mệnh lệnh của ai, họ đã đánh sập những gì, và đến mức nào.

Cách kéo tình nguyện viên vào một cuộc chiến không phải đến năm 2022 mới xuất hiện. Ukraine từng có một nhóm trinh sát bằng drone tình nguyện, Aerorozvidka, hoạt động từ năm 2014. Dân thường tiếp tục thử nghiệm việc gắn smartphone, máy tính bảng và drone bán thương mại vào các hoạt động quân sự, và một báo cáo công nghệ quân sự ghi nhận rằng những thử nghiệm này đã trở thành nền tảng ý tưởng của Delta, hệ thống nhận thức tình huống chiến trường của quân đội Ukraine, vào năm 2017.

Aerorozvidka và IT Army khác nhau ở cách họ kiểm chứng thông tin. Dữ liệu trinh sát của Aerorozvidka, giống như các báo cáo của công dân gửi qua chatbot eVorog, đi qua khâu kiểm chứng rồi chảy vào Delta. Thông tin có một tầng lọc, và có một hệ thống tiếp nhận rồi dùng nó. Không có khâu như vậy được ghi nhận trong hồ sơ công khai về các cuộc tấn công DDoS của IT Army. Mục tiêu được đưa xuống qua Telegram, còn việc chúng có được hành động theo hay không, và kết quả ra sao, vẫn nằm trên laptop của từng người.

Cũng cần nhìn vào nguồn gốc của những mục được liệt kê như thành tựu. Câu nói rằng mật khẩu quản trị của Rutube đã bị thay đổi và dữ liệu ở quy mô petabyte đã bị xóa là một ghi chép từ báo cáo của New Strategy Center. Trong hồ sơ công khai, không có tài liệu nào cho thấy phía Nga bị nhắm tới đã xác nhận thiệt hại đó. Một ghi chép chỉ do bên tấn công để lại, cùng với các báo cáo phân tích bên đó, không được đọc như thiệt hại đã được xác nhận.

Nhận xét rằng các ranh giới đã mờ đi không chỉ nằm trên mặt trận mạng. Người điều khiển drone, người chụp ảnh binh sĩ đối phương rồi tải lên mạng, và người dồn dập gửi yêu cầu kết nối vào máy chủ của người khác đều đã bước vào cùng một vùng xám. Việc Ukraine đưa họ vào trong khuôn khổ pháp luật hay để họ ở bên ngoài vẫn còn phụ thuộc vào một dự luật đang ở giai đoạn dự thảo, và trong lúc đó, cái giá được trả bởi từng tình nguyện viên cá nhân.

Chương 4. Mặc cả với Musk: Starlink

Ngày 26 tháng 2 năm 2022, Mykhailo Fedorov đã đề nghị Elon Musk trên X (khi đó là Twitter) gửi các thiết bị đầu cuối Starlink. Đó là một yêu cầu công khai, không đi qua công hàm ngoại giao và cũng không qua đại sứ quán. Musk trả lời, và hai ngày sau, ngày 28 tháng 2, lô thiết bị đầu cuối đầu tiên đã đến Ukraine.

Bài đăng đó thường được dẫn lại như ví dụ tiêu biểu cho cách Fedorov phản ứng trong những ngày đầu của chiến tranh. Câu chuyện thường được kể rằng một bộ trưởng trẻ đã nhờ Elon Musk giúp qua mạng xã hội và cứu hệ thống liên lạc của đất nước. Trên thực tế, nhiều chính phủ và tổ chức đã tham gia vào nỗ lực cung cấp này.

Chỉ riêng bài đăng công khai không giải thích được toàn bộ chuỗi cung cấp thiết bị đầu cuối. Vì sao internet vệ tinh được chọn, các thiết bị đầu cuối được dùng ở đâu, và Ukraine phải gánh những chi phí, điều kiện nào, tất cả đều phải được đối chiếu với các nguồn khác. Một tình huống trong đó điều khoản dịch vụ của một công ty tư nhân và phán đoán của một giám đốc duy nhất trên thực tế lại quyết định phạm vi liên lạc mà một quốc gia đang có chiến tranh có thể dùng, đó là vấn đề lần đầu tiên cuộc chiến này tạo ra. Vì vậy, Stockholm International Peace Research Institute (SIPRI), trong một báo cáo tháng 6 năm 2023, đã xem tác động của chiến tranh Ukraine đối với quản trị không gian như một chủ đề riêng.

Những trang này chủ yếu dựa trên một báo cáo do RAND Corporation công bố vào tháng 3 năm 2025. Các tuyến cung cấp thiết bị đầu cuối ban đầu, việc lắp đặt trong các cơ sở y tế, các trường hợp Bucha và đường sắt, cùng việc ghép nối với drone đều đến từ báo cáo đó. Khi có thể kiểm tra chéo, phần trình bày được bổ sung bằng báo cáo miltech do French Institute of International Relations (IFRI) và Munich Security Conference công bố tháng 2 năm 2026, bằng một thông báo của Ukrainian Ministry of Defence tháng 2 năm 2026, và bằng tin bài báo chí trong nước. Khi không thể kiểm tra chéo, chính câu văn sẽ nói rõ rằng nó dựa trên một nguồn duy nhất. Điều mà một báo cáo truyền đạt có khả năng là đúng, nhưng có khả năng đúng không giống với đã được xác lập.

1. Từ một lời kêu gọi công khai đến khi các thiết bị đầu cuối được đưa tới

Ngay trước khi cuộc xâm lược toàn diện bắt đầu, hệ thống thông tin liên lạc của Ukraine đã từng sụp đổ một lần. Vào đêm trước cuộc xâm lược, tin tặc Nga mở một cuộc tấn công quy mô lớn nhằm vào mạng KA-SAT của công ty thông tin vệ tinh Mỹ Viasat. Các đường truyền vệ tinh mà quân đội Ukraine và một số cơ quan chính phủ đang dựa vào bị tê liệt, khiến việc chỉ huy và kiểm soát trong những ngày đầu của cuộc chiến chịu áp lực nặng nề.

Cuộc tấn công Viasat thực sự làm tê liệt hệ thống chỉ huy và kiểm soát của Ukraine đến mức nào là điều được các tổ chức phân tích đánh giá khác nhau. Một số báo cáo xem đây là đòn

đánh quyết định trong giai đoạn mở màn; những báo cáo khác cho rằng quân đội Ukraine đã có sẵn các phương tiện liên lạc khác và tác động của cuộc tấn công chỉ có giới hạn. Việc cân nhắc các chứng cứ và phương pháp luận trái ngược nhau là việc dành cho một nơi khác. Sự kiện cần giữ lại ở đây thu hẹp vào một điểm. Cuối tháng 2 năm 2022, sau khi vừa thấy rõ thông tin vệ tinh có thể bị cắt đứt dễ dàng đến mức nào, chính phủ Ukraine bắt đầu tìm một tuyến thay thế.

Starlink là một dịch vụ cung cấp truy cập internet thông qua một mạng dày đặc gồm các vệ tinh nhỏ mà SpaceX đã đưa vào quỹ đạo Trái Đất tầm thấp. Cụm từ này còn lạ, nên cần giải thích rõ. Internet vệ tinh cho đến lúc đó thường có nghĩa là đưa một số ít vệ tinh lớn, đắt tiền lên quỹ đạo cao hơn nhiều. Vì vệ tinh ở vị trí cao, một vệ tinh có thể phủ một vùng rộng. Đổi lại, tín hiệu phải đi một quãng đường dài, nên phản hồi chậm; và nếu một trong số ít vệ tinh ấy bị vô hiệu hóa, cả một vùng rộng lớn sẽ mất kết nối cùng lúc. Đó là điều đã xảy ra khi Viasat bị nhắm tới. Các hệ thống quỹ đạo thấp nằm ở phía ngược lại. Mỗi vệ tinh nhỏ và có vòng đời ngắn, nhưng số lượng nhiều đến mức việc mất vài vệ tinh không làm dịch vụ dừng ngay. Trên mặt đất, chỉ cần một thiết bị đầu cuối dạng chảo và nguồn điện, không cần cáp quang, không cần trạm gốc, không cần trung tâm chuyển mạch.

Ở những khu vực mà pháo kích đã xóa sạch các cơ sở viễn thông, điều kiện đó mang tính quyết định. Xây lại các trạm gốc của một thành phố cần vật liệu, nhân công và thời gian, còn trạm gốc vừa xây lại vẫn có thể bị pháo kích lần nữa. Một thiết bị đầu cuối vệ tinh đứng ngoài vòng lặp đó. Một mạng lưới không có hạ tầng mặt đất để bị đánh sập, đó là thứ Ukraine đang tìm kiếm vào mùa xuân năm 2022.

Từ lúc bài đăng của Fedorov xuất hiện, đến câu trả lời của Musk, rồi đến khi thiết bị tới nơi vào ngày 28 tháng 2, chưa đầy ba ngày đã trôi qua. Đó là tốc độ mà không quy trình mua sắm nào của chính phủ có thể hình dung. Trong nhịp độ bình thường của bộ máy hành chính thời bình, chỉ riêng việc công bố hồ sơ mời thầu, đặt ra thông số kỹ thuật và ký hợp đồng đã mất nhiều tháng.

Dù vậy, nếu viết rằng một dòng tweet của một người đã tạo ra tốc độ ấy thì đã thu hẹp sự thật quá mức. Nguồn cung Starlink ban đầu không chỉ có SpaceX, mà còn có chính phủ United States, United States Agency for International Development (USAID), Poland và France. Chính các cơ quan và chính phủ này đã mua hàng nghìn thiết bị đầu cuối và vận chuyển chúng tới biên giới.

Những cuộc đàm phán nào thật sự đã diễn ra sau dòng tweet, ai quyết định điều gì và vào thời điểm nào, không thể được dựng lại từ các tài liệu đã công bố. Về những gì đã diễn ra giữa Fedorov và Musk, cũng như chính phủ United States đã can dự ở thời điểm nào và theo cách nào, hồ sơ gốc dừng lại tại đây. Những cuộc trao đổi và quyết định nằm ngoài hồ sơ công khai không được đưa vào văn bản này.

Điều nhìn thấy được là kết quả. Từ tháng 2 đến tháng 4 năm 2022, khoảng 5.000 thiết bị đầu cuối Starlink đã được đưa vào Ukraine, và trong thời gian đó tính liên tục của chuỗi chỉ huy quốc gia đã được khôi phục, theo ghi nhận trong báo cáo công nghệ quân sự của IFRI và Munich Security Conference. Cụm từ "tính liên tục của chuỗi chỉ huy" nghe cứng, nhưng ý nghĩa của nó không khó hiểu. Nó có nghĩa là chỉ thị từ văn phòng tổng thống đến được các chính quyền vùng, mệnh lệnh từ sở chỉ huy quân sự đến được các đơn vị cấp dưới, không bị đứt đoạn; và khi sự đứt đoạn ấy xảy ra, một nhà nước chỉ còn tồn tại trên bản đồ.

Người dùng tăng nhanh hơn nguồn cung. Năm tuần sau khi dịch vụ đi vào hoạt động, số người dùng Starlink hằng ngày bên trong Ukraine đã đạt 150.000, theo báo cáo của RAND. Con số ấy phải được xử lý thận trọng. Ai đã tổng hợp con số 150.000 và bằng cách nào, liệu nó đến từ nhật ký kết nối của SpaceX hay từ ước tính của chính phủ Ukraine, đó là nơi hồ sơ công khai trong báo cáo ấy dừng lại. 5.000 thiết bị đầu cuối trước đó và con số 150.000 này đến từ các nguồn khác nhau và các mốc tham chiếu khác nhau. Lấy số này chia cho số kia để nói mỗi thiết bị đầu cuối được bao nhiêu người dùng chung khó có thể gọi là một phương pháp chính xác, và tốt hơn là dừng lại ngay tại điểm nảy sinh cám dỗ làm phép tính ấy. Điều có thể xác nhận chỉ đến mức này. Vào thời điểm số thiết bị đầu cuối tính bằng hàng nghìn, số người dùng đã leo lên hàng trăm nghìn, và đến lúc đó Starlink đã vượt ra ngoài tính chất của một thiết bị thông tin quân sự.

Hình thức của lời đề nghị cũng định hình bản chất của mối quan hệ. Fedorov đã chọn một nền tảng công khai thay vì một kênh ngoại giao riêng. Bên đối ứng là một công ty chứ không phải một nhà nước, và giám đốc điều hành của công ty ấy là người phản ứng tức thì trên mạng xã hội. Một người bị nêu tên công khai rất khó giữ im lặng, vì không trả lời tự nó cũng là một câu trả lời. Áp lực này là một loại sức ép không được ghi trong bất kỳ hiệp ước hay hợp đồng nào. Đây không hẳn là một sự kiện nằm trong các tài liệu công khai, mà là cách tác giả đọc các tài liệu ấy.

Lựa chọn ấy đã phát huy tác dụng, đồng thời cũng ấn định bản chất của mối quan hệ. Lời đề nghị trở thành một phản hồi cá nhân chứ không phải một thỏa thuận giữa các nhà nước, và phản hồi ấy mang hình thức của một ân huệ. Điều bắt đầu như một ân huệ cũng có thể bị rút lại như một ân huệ. Mầm mống của vấn đề mà Ukraine sẽ đối mặt từ mùa thu năm 2022 nằm ở đây. Dù vậy, không có cơ sở để cho rằng vào cuối tháng 2 năm 2022 Ukraine có sẵn những lựa chọn khác một cách dễ dàng; trên thực tế chỉ có một nhà khai thác có thể cung cấp internet vệ tinh với số lượng lớn trong vòng vài ngày.

Tính chất của cuộc tấn công Viasat cũng đáng được lưu ý. Không có vệ tinh nào bị bắn hạ. Vào đêm trước cuộc xâm lược, tin tặc Nga xâm nhập qua nhiều tuyến cùng lúc, làm mạng KA-SAT tê liệt, và các liên kết vệ tinh bị cắt đứt mà không cần một quả bom nào. Ngay trong ngày đầu tiên của cuộc chiến, người ta đã thấy rõ rằng một mạng lưới có thể tối đen mà không bị phá hủy về

mặt vật lý.

Trong cùng giai đoạn đó, dữ liệu của đất nước được chuyển ra ngoài biên giới thông qua các thiết bị Snowball của Amazon Web Services và đám mây Azure của Microsoft. Quy mô và quy trình đã được trình bày ở Chương 2. Điều cần nói ở đây là các chảo thu thuộc về SpaceX, còn các máy chủ thuộc về Amazon và Microsoft. Nền móng để nhà nước đứng vững đã dịch chuyển sang cơ sở hạ tầng của các công ty tư nhân nước ngoài.

Các công chức và nhà phát triển thực hiện công việc trong mười tuần trích xuất dữ liệu ấy đã làm việc trong điều kiện nào, và các thiết bị lưu trữ đã đi qua biên giới theo tuyến nào, không được ghi lại trong những tài liệu công khai hiện có.

2. Một mạng vệ tinh tư nhân kết nối bệnh viện, chính phủ và tiền tuyến

Các thiết bị đầu cuối Starlink không chỉ được lắp đặt ở tiền tuyến mà còn trong những bệnh viện đã mất kết nối. Bộ Y tế Ukraine cho biết trong vòng một tháng kể từ khi dịch vụ bắt đầu, họ đã lắp Starlink tại 590 cơ sở y tế. Con số đó là thống kê riêng của một bộ thuộc chính phủ Ukraine, và báo cáo RAND đang thuật lại thông báo ấy. Số thiết bị đã lắp có khớp với số thiết bị thật sự hoạt động hay không, và các kết nối đó duy trì được bao lâu, là chỗ hồ sơ công khai dừng lại. Thay vì chép lại một thông báo của chính phủ như sự thật đã được kiểm chứng, cách chính xác hơn là nêu rõ ai đã công bố và đó là loại thông báo gì.

Vì sao truy cập internet lại quan trọng trong bệnh viện có lẽ cần được giải thích. Một bệnh viện hiện đại xử lý hồ sơ bệnh nhân, kho thuốc, việc chuyển tuyến và tiếp nhận bệnh nhân, cùng việc chia sẻ kết quả xét nghiệm qua mạng dữ liệu. Khi đường truyền bị đứt, bác sĩ không thể xem tiền sử của bệnh nhân, cũng không thể chuyển bệnh nhân đi nơi khác hay tiếp nhận bệnh nhân từ nơi khác. Tại một bệnh viện gần tiền tuyến, một đường dây bị cắt không chỉ gây bất tiện hành chính mà trở thành vấn đề sống còn.

Việc sửa chữa hạ tầng dân sự cũng bắt đầu ngay lập tức. Tại Bucha, bên ngoài Kyiv, nhà mạng di động Lifecell đã dùng Starlink để khôi phục một phần các dịch vụ di động bị phá hủy. Các lãnh đạo của công ty đường sắt nhà nước Ukrzaliznytsia duy trì kết nối qua Starlink trên những đoàn tàu đang chạy, rồi từ đó chỉ đạo logistics đường sắt và việc di chuyển của người tị nạn. Cả hai trường hợp đều đến từ một báo cáo RAND duy nhất và chưa được đối chiếu với các nguồn khác.

Đường sắt và mạng di động là hạ tầng dân sự, nhưng trong thời chiến chúng cũng chuyên chở sự cơ động và liên lạc quân sự. Dù vậy, vào mùa xuân năm 2022, khi hàng triệu người đang di chuyển về phía biên giới phía tây, lịch tàu và mạng điện thoại là điều kiện để sống sót. Biết đoàn tàu dừng ở ga nào và tuyến liên lạc nào vẫn còn hoạt động, so với không biết gì, tạo ra khác biệt rất lớn. Trong những tuần đầu của cuộc chiến, quyền tiếp cận thông tin liên quan trực tiếp đến việc ngăn hoảng loạn trong dân chúng, cùng báo cáo ấy ghi nhận. Hoảng loạn tự nó

tạo ra hệ quả quân sự, vì khi đường bộ bị nghẽn bởi các đoàn người tị nạn, xe tiếp tế cũng không thể đi qua.

Theo thời gian, trọng tâm của Starlink đã dịch chuyển từ hậu phương ra tiền tuyến. Đến đầu năm 2023, khoảng 42.000 thiết bị đầu cuối đang hoạt động ở Ukraine, tăng hơn tám lần chỉ trong một năm.

Các chảo thu được đặt trong chiến hào, trong hầm trú ẩn và trong nơi che chắn xe bọc thép. Các chỉ huy phối hợp chiến dịch qua những đường truyền thời gian thực được mã hóa và chuyển tọa độ địch cho các đơn vị pháo binh. Việc chuyển tọa độ đến khẩu đội mất vài phút hay chỉ vài chục giây quyết định mục tiêu còn ở đó hay không. Với một mục tiêu đang di chuyển, độ trễ liên lạc là một cách nói khác của độ chính xác.

Sự kết hợp với drone còn đi xa hơn một bước. Các thiết bị đầu cuối Starlink được gắn trực tiếp lên thân drone. Bằng cách trao đổi video và dữ liệu trực tiếp qua đường truyền vệ tinh, người điều khiển có thể nhận diện mục tiêu ngoài tầm nhìn thẳng và hỗ trợ các đòn tấn công chính xác vào ban đêm.

Quy mô của thay đổi này thể hiện ở bán kính hoạt động. Trước đó, bán kính của một drone bị ràng buộc bởi khoảng cách mà tín hiệu vô tuyến điều khiển có thể vươn tới, tức giới hạn của các trạm chuyển tiếp mặt đất và ăng-ten. Chỉ cần một ngọn đồi chặn tín hiệu, mọi việc kết thúc tại đó. Đường truyền vệ tinh vòng qua giới hạn ấy bằng cách đi lên cao, vì tín hiệu không đi theo địa hình mà quay trở lại qua bầu trời. Người ta thường nói drone giá rẻ đã làm thay đổi cuộc chiến; thứ đưa những chiếc drone ấy bay xa lại là một mạng lưới vệ tinh không hề rẻ.

Ban đầu, Starlink xuất hiện như một lớp bảo đảm chiến lược, một đường truyền dự phòng để dùng khi các mạng hiện có sụp đổ. Đến năm 2023, Starlink đã vượt khỏi vai trò đường truyền dự phòng và trở thành một phụ thuộc chiến thuật, thứ mà các đơn vị dựa vào về mặt cấu trúc để chỉ huy hỏa lực pháo binh và điều khiển drone. Mất một đường truyền dự phòng chỉ gây bất tiện; khi một phụ thuộc bị cắt, chiến dịch dừng lại.

Điểm yếu của một dịch vụ thương mại dành cho người tiêu dùng là bất kỳ ai cũng có thể mua nó. Khi chiến tranh kéo dài, lực lượng Nga cũng bắt đầu dùng các thiết bị đầu cuối Starlink được tuồn vào chiến trường qua các nước thứ ba. Các bộ phận Starlink đã được nhận diện trong đống đổ nát của đạn bay lảng vảng Shahed dựa trên thiết kế Iran và của drone Molniya. Mạng lưới mà Ukraine đã hồi sinh quay trở lại như đường liên lạc cho những drone tấn công các thành phố Ukraine.

Phản ứng đến từ cả phía kỹ thuật lẫn phía hành chính. Về kỹ thuật, SpaceX áp dụng geofencing, một chức năng tự động chặn dịch vụ theo vị trí và điều kiện. Nếu một thân máy bay mang thiết bị đầu cuối Starlink bị phát hiện bay nhanh hơn 75 đến 90 kilomet một giờ, kết nối của thiết bị đó bị cắt. Theo truyền thông trong nước, các drone Nga bay về phía hậu phương

mất liên kết và bị vô hiệu hóa. Một thiết bị đầu cuối do người mang hoặc gắn trên xe hiếm khi vượt quá tốc độ đó; một loại đạn bay lảng vảng thì có. Một đại lượng vật lý duy nhất, tốc độ, đã tách người dùng dân sự khỏi vũ khí tấn công.

Về hành chính, Bộ Quốc phòng Ukraine đưa ra hệ thống danh sách trắng, một biện pháp theo đó chỉ các thiết bị đầu cuối đã được chứng nhận và đăng ký mới hoạt động trên lãnh thổ Ukraine. Người dùng phải kiểm tra số KIT và mã định danh UTID của thiết bị đầu cuối rồi hoàn tất đăng ký; thiết bị chưa đăng ký sẽ bị cắt khỏi mạng. Ngay cả các thiết bị đã được phê duyệt cũng chỉ được phép hoạt động khi đứng yên hoặc di chuyển ở tốc độ thấp. Bộ này công bố việc đó vào ngày 3 tháng 2 năm 2026, và các cơ quan truyền thông trong nước đưa tin cùng diễn biến này vào ngày 5 tháng 2 năm 2026.

Mốc thời gian này đáng được ghi lại. Tháng 2 năm 2026 rơi vào sau thời điểm Fedorov tiếp quản Bộ Quốc phòng. Nhưng việc ông đề xuất hay phê chuẩn hệ thống này là điểm mà hồ sơ công khai trong những tài liệu hiện có dừng lại. Một thông báo của bộ sẽ được giữ đúng là một thông báo của bộ. Chép lại mọi việc một bộ đã làm trong nhiệm kỳ của một bộ trưởng thành thành tích cá nhân của vị bộ trưởng ấy là cái bẫy mà tiểu sử thường mắc phải.

Hướng đi của hệ thống thì rõ. Thiết bị mà bất kỳ ai cũng có thể mua và bật lên nay chỉ bật được sau khi được đưa vào sổ đăng ký của Bộ Quốc phòng; sự tiện lợi thu hẹp lại, còn kiểm soát tăng lên. Chiến tranh đại khái làm như vậy với công nghệ dân sự.

Tính đến ngày tham chiếu 13 July 2026, các bản tin xác nhận rằng những nỗ lực gây nhiễu và né tránh của Nga, cùng các biện pháp đáp trả của Ukraine và SpaceX, vẫn tiếp diễn theo nhịp luân phiên. Cuộc đấu giữa giáo và khiên vẫn chưa đi đến dấu chấm hết.

Câu nói rằng một mạng vệ tinh tư nhân đã kết nối bệnh viện, chính phủ và tiền tuyến là đúng. Nhưng chính câu đó cũng có thể đọc ngược lại. Nó còn có nghĩa là bệnh viện, chính phủ và tiền tuyến đã bị buộc vào một dịch vụ duy nhất của một công ty tư nhân duy nhất. Mạng lưới ấy không được dựng nên bởi một dòng tweet, mà bởi hàng nghìn bàn tay; tuy vậy, công tắc bật tắt mạng lưới đó lại nằm ở một nơi.

Cần nhìn kỹ hơn một chút vào những gì danh sách trắng đòi hỏi ở người dùng. Chủ sở hữu thiết bị đầu cuối phải tìm số KIT và mã định danh UTID của thiết bị, rồi hoàn tất chứng nhận theo hướng dẫn của bộ; thiết bị chưa được chứng nhận sẽ bị cắt kết nối. Ngay cả thiết bị đã được chứng nhận cũng chỉ hoạt động khi đứng yên hoặc di chuyển chậm. Việc đăng ký được xử lý ra sao đối với người dùng ngoài quân đội như bệnh viện hoặc tổ chức cứu trợ, và có thủ tục khiếu nại nào khi đăng ký bị từ chối hay không, đều không được ghi trong thông báo.

Việc chia theo tốc độ có một điểm vướng. Các thiết bị đầu cuối Starlink cũng từng được gắn lên khung thân drone của Ukraine. Một quy định cắt liên kết của một khung bay tốc độ cao vận hành song song thế nào với một thực tế tác chiến gắn thiết bị đầu cuối lên chính các khung bay

tốc độ cao ấy, điều đó không xuất hiện trong thông báo của bộ, cũng không có trong báo cáo RAND. Có ngoại lệ riêng cho liên kết quân sự hay không, hoặc có một cơ chế chứng nhận tách biệt hay không, là nơi hồ sơ công khai dừng lại.

Chính phủ Ukraine và một công ty tư nhân, mỗi bên đều định hình phạm vi của dịch vụ. Một ràng buộc do SpaceX áp đặt bằng geofencing; ràng buộc kia do Bộ Quốc phòng Ukraine áp đặt thông qua đăng ký. Điều công ty đặt ra thì công ty gỡ bỏ; điều bộ đặt ra thì bộ gỡ bỏ. Khi quyền kiểm soát tăng lên, số bàn tay tham gia kiểm soát cũng tăng theo. Việc một biện pháp chống drone Nga đồng thời trở thành một biện pháp quản lý chính công dân của mình là kết quả của việc đọc hai biện pháp chồng lên nhau, chứ không phải là một câu được văn bản nào ghi ra.

3. Việc cắt kết nối Crimea và tranh chấp chi phí: Điều khoản của một công ty trở thành địa chính trị

Vào mùa thu năm 2022, lực lượng Ukraine đã đưa các phương tiện mặt nước không người lái vào Biển Đen. Mục tiêu là Hạm đội Biển Đen của Nga đang neo ngoài khơi Sevastopol, tại Crimea. Trong phạm vi hoạt động, kết nối Starlink không thiết lập được; các xuồng drone mất liên lạc, trôi dạt vào bờ, và chiến dịch thất bại.

Từ đó đến nay, vụ việc này được kể lại theo nhiều phiên bản mâu thuẫn nhau. Chỉ dựa vào các tài liệu đã công bố, rất khó xác định bản tường thuật nào là đúng.

Báo cáo của RAND và một số cơ quan báo chí nói rằng chính phủ Ukraine đã khẩn cấp yêu cầu mở dịch vụ Starlink đến tận Sevastopol và Musk đã từ chối. Bản thân Musk, trong một bài đăng trên X, nói rằng ý định của Ukraine là đánh chìm hạm đội Nga khi đang neo đậu, và nếu ông chấp thuận yêu cầu đó thì SpaceX sẽ trở thành bên đồng lõa trong một hành động chiến tranh lớn và trong việc làm leo thang xung đột. Ông nêu lý do lo ngại rằng việc đó có thể lan thành chiến tranh hạt nhân.

"Một dịch vụ đã được bật rồi bị tắt đi" và "một yêu cầu bật dịch vụ đã bị từ chối" là hai câu chuyện khác nhau. Nếu cách hiểu thứ nhất đúng, một công ty đã chặn một chiến dịch đang diễn ra; nếu cách hiểu thứ hai đúng, một công ty đã từ chối yêu cầu mở rộng khu vực dịch vụ của mình. Sức nặng đạo đức và hệ quả pháp lý của hai việc này không giống nhau. Bản thân Musk khẳng định cách hiểu thứ hai, còn có những hồ sơ lại trình bày vụ việc theo cách thứ nhất. Đâu là sự thật, và chính phủ Hoa Kỳ hay các bên khác đã tác động thế nào đến phán đoán đó, là điều không thể kết luận từ các tài liệu đã công bố.

Bản tường thuật này sẽ không đi sâu vào động cơ bên trong của Musk. Có những lời đồn xoay quanh việc liệu ông có lợi ích thương mại đang bị ảnh hưởng hay không, hoặc đã có những liên hệ nào với phía Nga hay không, nhưng dựa trên các tài liệu hiện có, hồ sơ công khai dừng lại ở đây. Ngay khi người viết trình bày những điều nằm ngoài hồ sơ công khai như thể đã được xác nhận, tiểu sử sẽ biến thành hư cấu.

Điều có thể thấy là kết quả và cấu trúc. Kết quả là một chiến dịch thất bại, còn cấu trúc là thế này. Phạm vi mà một quốc gia tham chiến có thể tiến hành hoạt động quân sự trên thực tế lại do vùng phủ dịch vụ của một công ty tư nhân ấn định. Baroness Martha Lane Fox, thành viên British House of Lords, đã chỉ trích cách sắp đặt này, nói rằng quyền kiểm soát Starlink chỉ nằm trong tay Elon Musk và phán đoán của ông quyết định quyền tiếp cận hạ tầng trọng yếu.

Giữa các quốc gia có hiệp ước, và hiệp ước có thủ tục. Nếu hiệp ước bị vi phạm, vẫn có chỗ để tranh cãi, và cách tranh cãi đã được quy định sẵn. Điều khoản dịch vụ của một công ty thì không có gì tương tự. Khu vực nào được cung cấp dịch vụ, cách dùng nào được cho phép, khi nào dịch vụ bị đình chỉ, công ty quyết định. Trong thế giới hợp đồng thương mại, đó là một thẩm quyền tự nhiên. Một dịch vụ video hoạt động ở nước nào và không hoạt động ở nước nào là quyết định của công ty, và không ai gọi đó là hành vi vi phạm chủ quyền.

Khi dịch vụ đó là đường truyền chỉ huy và kiểm soát của một quốc gia đang có chiến tranh, chính thẩm quyền ấy trở thành một quyết định địa chính trị và một hành động kẻ đường trên bản đồ. Đó là nơi báo cáo tháng 6 năm 2023 của SIPRI đặt cuộc chiến ở Ukraine vào vấn đề quản trị không gian. Hiện vẫn chưa có thỏa thuận nào về việc luật pháp và chuẩn mực quốc tế được áp dụng đến đâu khi một nhà khai thác không gian tư nhân tham gia sâu vào xung đột vũ trang, hoặc liệu một nhà khai thác như vậy có thể được xem là một bên trong xung đột hay không. Không có thỏa thuận thì không có chỗ để đưa ra phán quyết, và nơi không có chỗ để phán xét, quyết định quay trở lại với bất cứ ai có khả năng quyết định.

Cùng với tranh chấp về quyền kiểm soát là tranh chấp về chi phí. Trong giai đoạn đầu, SpaceX tự gánh hơn 80 triệu dollars. Khi số người dùng và thiết bị đầu cuối tăng lên, gánh nặng trở nên khó chịu đựng, Musk đã đề nghị US Department of Defense cấp kinh phí.

Chi phí được chia sẻ giữa một số chính phủ. USAID, Poland, France và các bên khác đảm nhận việc mua và chuyển giao hàng nghìn thiết bị đầu cuối. Chính phủ Germany phân bổ 20 triệu euros để chi trả phí dịch vụ Starlink của Ukraine. US Department of Defense ký một hợp đồng sáu tháng với SpaceX trị giá 14 triệu dollars, giúp nguồn cung dịch vụ ổn định hơn.

Câu chuyện rằng "Musk đã tặng internet cho Ukraine" chỉ giải thích được một phần trong vài tháng đầu. Một phần đáng kể hoạt động của Starlink được duy trì bằng ngân sách của các chính phủ phương Tây, và cách hiểu sát với thực tế hơn là nó bắt đầu như một khoản quyên tặng rồi chuyển thành hợp đồng. Quyền kiểm soát cũng không chuyển sang tay các chính phủ sau khi họ bắt đầu thanh toán hóa đơn. Việc bên trả tiền và bên giữ công tắc là hai bên khác nhau chính là điểm cốt lõi của cách sắp đặt này, và một hợp đồng trong đó bên trả tiền không thể đặt ra điều kiện sử dụng không phải là chuyện thường gặp. Hoàn cảnh chiến tranh đã tạo ra hợp đồng khác thường đó.

Ukraine không ngồi yên. Các nỗ lực nhằm giảm lệ thuộc vào một công ty duy nhất đã nối tiếp nhau xuất hiện. Dịch vụ của nhà khai thác vệ tinh OneWeb được đưa vào, và với nguồn tài trợ

của chính phủ Germany, một kế hoạch được lập ra để triển khai từ 5.000 đến nhiều nhất 10.000 thiết bị đầu cuối OneWeb tại Ukraine. Phần có thể xác nhận chỉ dừng ở kế hoạch và khoản phân bổ kinh phí. Hồ sơ công khai dừng lại ở chỗ thiếu các tài liệu cho thấy thực tế đã triển khai bao nhiêu thiết bị và bao nhiêu thiết bị hoạt động được.

OneWeb không thể thay thế Starlink. Thiết bị đầu cuối của họ lớn, và không được tinh chỉnh cho hoạt động quân sự. Dù vậy, hướng đi đã rõ: loại bỏ điểm lỗi duy nhất, tức thứ mà một khi sụp đổ sẽ kéo mọi thứ sụp theo, và giành lại quyền tự chủ chính trị. Như báo cáo của IFRI diễn đạt, đó là nỗ lực tiến tới một hệ sinh thái liên lạc lai, pha trộn nhiều quỹ đạo và nhiều nhà khai thác. Hiệu quả giảm, chi phí tăng, và đó là cái giá của quyền tự chủ.

Vậy nên đánh giá bài đăng ngày 26 tháng 2 năm 2022 ấy như thế nào?

Công lao thì rõ. Trong một đất nước mà hệ thống liên lạc đã sụp đổ, nó nén vào vài ngày việc mà nếu theo mua sắm công của chính phủ có lẽ phải mất nhiều tháng. Nó chọn đúng mục tiêu để đưa ra yêu cầu, và dùng một nền tảng công khai làm công cụ gây sức ép. 590 cơ sở y tế được Bộ Y tế thống kê và 42.000 thiết bị đầu cuối vào đầu năm 2023 đều là những phần của một dòng chảy bắt đầu từ lựa chọn đó.

Sai sót cũng rõ. Có lẽ gọi đó là cái giá thì chính xác hơn là sai sót. Khi xây tầng liên lạc của một quốc gia trên một ân huệ, đến lúc ân huệ ấy nguội đi thì không còn gì để dựa vào. Những chiếc thuyền drone dạt vào bờ ngoài khơi Crimea chính là khoảnh khắc cái giá ấy đến hạn phải trả.

Hai câu ấy phải được đặt cạnh nhau. Không có cơ sở để cho rằng Fedorov cũng tự mình thiết kế cả những hệ quả về sau. Cũng không có cơ sở để cho rằng Ukraine vào tháng 2 năm 2022 có những lựa chọn thay thế dễ chịu. Thành quả do việc hành động thật nhanh tạo ra, và sự phụ thuộc mà cách hành động ấy để lại, là mặt trước và mặt sau của cùng một sự kiện. Chỉ nhìn một mặt rồi viết thành câu chuyện anh hùng, hoặc viết thành bản cáo trạng về sai lầm, đều dễ làm và đều không chính xác.

Xây dựng một mặt trận số trên hạ tầng dân sự có nghĩa là gì, đó là câu hỏi mà các tổ chức chính sách, trong đó có Atlantic Council, vẫn đang đặt ra khi cuộc chiến đã bước sang năm thứ tư. Câu trả lời vẫn chưa xuất hiện. Nhiều quốc gia đang đứng trước cùng câu hỏi ấy. Bất cứ quốc gia nào đã đặt hệ thống hành chính và liên lạc quân sự của mình lên trên internet vệ tinh, dịch vụ đám mây, dịch vụ bản đồ và các ứng dụng nhắn tin đều ở trong cùng tình thế. Trong thời bình, điều đó không nhìn thấy được; đến khi nó hiện ra, thường đã muộn.

Trong hồ sơ về Fedorov, Starlink được nhớ đến như một phương pháp: nhanh chóng kéo từ bên ngoài nhà nước vào những thứ nhà nước không có. Con người, tiền bạc, công nghệ, tất cả được gọi tới từ bên ngoài nhà nước. Ngữ pháp ấy đã vận hành được trong chiến tranh. Nhưng ngữ pháp ấy để lại gì trong một nhà nước, đó là câu hỏi phải được đặt riêng.

Chi phí mua các thiết bị đầu cuối đã có trong hồ sơ, nhưng quá trình ấn định phạm vi phủ sóng của dịch vụ thì chưa bao giờ được công bố. Hợp đồng sáu tháng trị giá 14 triệu đô la của Pentagon với SpaceX và khoản 20 triệu euro của chính phủ Đức đã được xác nhận về mặt số tiền. Nhưng các hợp đồng ấy xác định khu vực dịch vụ, mục đích sử dụng được phép và điều kiện đình chỉ như thế nào, hoặc có xác định những điều đó hay không, thì hồ sơ công khai trong các tài liệu đã công bố dừng lại ở đó. Điều này có nghĩa là chúng ta không thể biết bên trả tiền có góp phần đặt ra các điều khoản hay không; và lý do không có chỗ để tranh cãi bằng tài liệu về quyết định được đưa ra ngoài khơi Sevastopol cũng nằm chính trong khoảng trống ấy.

OneWeb là một nhà khai thác vệ tinh có trụ sở tại Pháp, và nguồn tiền để triển khai tại Ukraine đến từ chính phủ Đức. Việc bổ sung thêm nhà khai thác làm giảm khả năng toàn bộ chiến dịch bị treo trên một phán đoán duy nhất của một công ty. Mức giảm rủi ro chỉ đến đó. OneWeb cũng là một công ty tư nhân, và bên trả tiền cho các thiết bị đầu cuối vẫn là một chính phủ nước ngoài. Dựa vào nhiều công ty và không dựa vào bên nào cả là hai chuyện khác nhau.

Lý do các phiên bản về sự cố Crimea khác nhau cũng nằm ở hình dạng của các tài liệu. Tuyên bố chính còn lại là một bài đăng do chính Musk đưa lên X, và chưa có hồ sơ nào do SpaceX hoặc chính phủ Mỹ để lại được công bố. Khi tuyên bố sau sự việc của một bên là tài liệu gốc duy nhất, đó là lời kể, không phải hồ sơ. Chương này đặt hai phiên bản cạnh nhau rồi dừng lại ở đó, không phải vì thận trọng, mà vì không còn tài liệu nào khác để bước tiếp.

Chương 5. Chiến tranh mạng thật sự đã thay đổi điều gì?

Ngày 24 tháng 2 năm 2022, dịch vụ internet vệ tinh của Viasat đồng loạt ngừng hoạt động tại sáu nước châu Âu. Hàng nghìn thuê bao mất kết nối ở Đức, Pháp, Hungary, Hy Lạp, Italy và Ba Lan. Thiệt hại lan tới cả những nước cách tiền tuyến hàng trăm kilômét.

Hơn 5.800 tua-bin gió do công ty năng lượng Đức Enercon quản lý cũng mất liên lạc từ xa. Các modem vệ tinh nối những tua-bin này với phòng điều khiển đã bị cuốn vào cuộc tấn công.

Cũng trong buổi sáng đó, lực lượng mặt đất của Nga vượt qua biên giới Ukraine. Một số báo cáo phân tích đặt khoảng cách thời gian giữa hai sự kiện là một giờ. Một giờ trước khi lực lượng mặt đất vượt biên, mạng KA-SAT của công ty truyền thông vệ tinh Mỹ Viasat đã bị tấn công mạng.

Mọi việc Fedorov thúc đẩy trong tuần đầu tiên của cuộc xâm lược đều dựa trên một điều kiện duy nhất: Nga có thể làm gì và không thể làm gì trong không gian mạng. Nếu không hình dung được quy mô của điều kiện ấy, rất khó đánh giá vì sao ông hành động gấp đến vậy, và ngay cả bây giờ vẫn còn quá sớm để khẳng định quy mô đó một cách chắc chắn.

Trước chiến tranh, các chuyên gia an ninh mạng trên khắp thế giới dự đoán các cuộc tấn công của Nga sẽ làm Ukraine sụp đổ trong vài ngày. Dự đoán ấy đã sai. Vì sao nó sai, và liệu nó có thật sự sai hay không, đến nay vẫn là vấn đề được các nhà phân tích tranh luận. Cuộc tranh luận chia thành ba điểm: quy mô của đòn đánh đầu tiên, quan hệ giữa tác chiến mạng và tên lửa, và thành công hay thất bại của chiến tranh mạng Nga.

1. Cuộc tranh cãi về mức thiệt hại mà vụ hack Viasat gây ra

Vụ hack Viasat có một giai đoạn chuẩn bị. Khó có thể xem đó là một cuộc phục kích bất ngờ xuất hiện từ hư không vào buổi sáng hôm ấy. Một báo cáo nghiên cứu về an ninh mạng thời chiến của Ukraine (ARMG Publishing) có phần 'dòng thời gian cuộc tấn công mạng Viasat'. Từ đầu tháng 2 năm 2022, khi quân Nga tiến về biên giới và căng thẳng tăng lên, các cuộc tấn công mạng nhắm vào hạ tầng trọng yếu và mạng lưới chính phủ của Ukraine bắt đầu xuất hiện. Ngày 23 tháng 2, một ngày trước cuộc xâm lược, các cuộc tấn công từ chối dịch vụ phân tán (DDoS) đánh vào ngân hàng và website chính phủ. Cách làm này dồn các yêu cầu kết nối vào một website từ nhiều máy tính cùng lúc cho đến khi máy chủ bị nghẽn, giống cảnh xếp hàng hàng chục nghìn khách hàng giả trước quầy ngân hàng để khách hàng thật không thể bước vào hơn.

Rồi đến ngày 24 tháng 2. Mã độc có tên AcidRain đi qua mạng vệ tinh KA-SAT xuống các modem và router dưới mặt đất. AcidRain được xếp vào nhóm wiper, tức công cụ xóa dữ liệu bên trong thiết bị. Nó không giống một tên trộm chọn món để lấy, mà giống một kẻ phóng hỏa phá hủy mọi thứ còn lại. Cuộc tấn công làm hàng nghìn modem và router mất kết nối, đồng

thời cắt đứt một trụ cột của mạng thông tin liên lạc mà quân đội, chính phủ và dân thường Ukraine cùng dùng.

Tên gọi và danh tính của công cụ này chỉ lộ ra một tháng sau sự kiện. Cuối tháng 3 năm 2022, công ty bảo mật SentinelOne xác nhận rằng công cụ đã xóa firmware của các thiết bị và làm chúng tê liệt là AcidRain. Firmware là phần mềm nằm ở tầng thấp nhất của một cỗ máy, lớp mà nó dùng để tự bật lên và vận hành. Xóa lớp đó đi, cỗ máy chỉ còn là một cái vỏ: bấm nút nguồn, nó không còn nhớ mình được tạo ra để làm gì.

Không khó giải thích vì sao thiệt hại lan ra ngoài Ukraine. Internet không nhìn biên giới. KA-SAT không chỉ phục vụ người dùng Ukraine. Thuê bao từ nhiều nước châu Âu cùng nằm dưới một mạng vệ tinh, vì vậy một cuộc tấn công nhắm vào liên lạc quân sự của Ukraine cũng làm các tuabin gió ở Đức ngừng hoạt động. Các báo cáo gọi hiện tượng này là 'international spillover'.

Khi thiệt hại lan qua nhiều quốc gia, vụ việc trở thành vấn đề ngoại giao. Ngày 10 tháng 5 năm 2022, Liên minh châu Âu, Hoa Kỳ, Vương quốc Anh và các nước khác ra tuyên bố chính thức, nêu tên cơ quan tình báo quân sự Nga, GRU, là bên đứng sau vụ hack. Nhiều chính phủ cùng chỉ ra một thủ phạm.

Đến đây, các sự kiện về cơ bản đã được đồng thuận. Có dấu thời gian, có tên của mã độc, có số lượng thiết bị bị hỏng, và có kết luận quy trách nhiệm chung từ nhiều chính phủ. Tranh cãi bắt đầu ở câu hỏi tiếp theo: cuộc tấn công này thật sự giáng một đòn lớn đến mức nào vào Ukraine. Ở câu hỏi đó, câu chuyện tách thành hai cách đọc.

Những bài tường thuật ban đầu mô tả sự cố này là một 'tổn thất liên lạc khổng lồ'. Tiêu đề của một bản tin Reuters ngày 15 March 2022 tiêu biểu cho cách hiểu đó. Bản tin nói rằng sự cố gián đoạn vệ tinh đã gây ra một tổn thất liên lạc khổng lồ khi chiến tranh bùng nổ, và căn cứ của nhận định này là tuyên bố của một quan chức Ukraine. Bài viết để lại cho thế giới ấn tượng rằng đòn tấn công đầu tiên của Russia đã giáng một vết thương chí mạng vào hệ thống chỉ huy và kiểm soát quân sự của Ukraine.

Một trong những người khiến cách hiểu này có thêm sức nặng là nhà phân tích Jon Bateman. Ông chỉ ra vụ hack Viasat như một trường hợp rõ ràng về hành động phá hoại có phối hợp trong miền thông tin. Căn cứ của ông gồm ba điểm: thời điểm xảy ra, một giờ trước khi lực lượng trên bộ vượt biên giới; mục đích quân sự rõ ràng là làm suy giảm năng lực liên lạc của Ukraine; và tác động lan ra quốc tế, làm rung chuyển kết nối ở nhiều nước European. Đặt ba điểm ấy cạnh nhau, rất khó gọi đó là trùng hợp.

Nửa năm sau, một cách thuật lại khác xuất hiện. Ngày 26 September 2022, phóng viên Kim Zetter đăng một bài trên cơ quan điều tra Zero Day. Bài viết cho biết một quan chức đã nói rằng vụ hack Viasat 'không' gây tác động khổng lồ đối với liên lạc quân sự của Ukraine.

Quan chức đó là Victor Zhora, một nhân vật cấp cao tại State Service of Special Communications and Information Protection (SSSCIP) của Ukraine. Ông thừa nhận rằng liên lạc quả thực đã bị cắt tạm thời trong những giờ đầu của cuộc xâm lược. Nhưng ông nói rằng nhờ tính 'dự phòng' đã được xây sẵn trong hệ thống liên lạc của Ukraine, sự cố này không gây tàn phá như người ta từng lo sợ.

Dự phòng nghĩa là thiết kế sẵn nhiều lớp, để nếu một tuyến liên lạc bị cắt, lưu lượng có thể chuyển sang tuyến khác. Một thành phố chỉ có một cây cầu sẽ bị cô lập khi cây cầu ấy sập; một thành phố có bốn cây cầu thì khi mất một cây, vẫn còn đường đi. Lập luận của Zhora là như thế này: ngay cả khi mạng Viasat bị xóa sổ, quân đội Ukraine đã chuyển sang các phương tiện khác, nên tình trạng tê liệt chỉ huy và kiểm soát mà Nga nhắm tới đã không xảy ra.

Cả hai phát biểu đều đến từ cùng một chính phủ Ukraine, nhưng chúng mô tả quy mô thiệt hại theo hai cách khác nhau. Người nói về một "tổn thất khổng lồ" vào tháng 3 là một quan chức Ukraine, và người nói vào tháng 9 rằng "không tệ đến mức đó" cũng là một quan chức Ukraine.

Lời lẽ chính thức của một quốc gia đang có chiến tranh trước hết là một hành động, rồi sau đó mới là một bản tường thuật sự thật. Khi cần kéo thêm viện trợ vũ khí, và khi cần cho thấy sức chịu đựng của quốc gia, quy mô của cùng một sự kiện có thể được mô tả khác đi. Tháng 3, Ukraine là một quốc gia đang xin thế giới giúp đỡ. Tháng 9, đó là một quốc gia đang trụ vững và chuẩn bị phản công.

Hồ sơ công khai chỉ đi xa đến đó. Giữa hai phát biểu ấy đã có điều chỉnh chính trị nào, hay ý định nào đã định hình cách Zhora cân chỉnh lời nói của mình, thì hồ sơ công khai dừng lại ở đây. Hai quan chức ấy có mâu thuẫn với nhau hay không, hồ sơ công khai cũng dừng lại ở đây. Điều có thể xác nhận là thời điểm và nội dung của các phát biểu, cùng sự thật rằng hai phát biểu ấy va thẳng vào nhau. Đi xa hơn nữa sẽ thành hư cấu.

Một phân tích của CNA đặt sự lẫn lộn này vào một khó khăn quen thuộc: các đánh giá về tác động của một cuộc tấn công mạng thường khác nhau khi kết luận được đưa ra trong lúc người ta chỉ có trong tay những bằng chứng ban đầu, chưa đầy đủ. Đó không hẳn là một chú thích gắn với riêng một sự kiện, mà giống một nhãn cảnh báo dán lên toàn bộ lĩnh vực phân tích chiến tranh mạng.

Nhãn cảnh báo ấy có lý do của nó. Tác động của một cuộc tấn công mạng không thể được đếm bằng ảnh chụp như một tòa nhà bị ném bom. Một khối chung cư sụp đổ còn có các tầng để đếm; một xe tăng bị phá hủy để lại xác xe. Nhưng đơn vị nào mất liên lạc trong bao nhiêu giờ, và trong thời gian đó mệnh lệnh nào không đến được nơi cần đến, lại là bí mật quân sự. Nếu nạn nhân không công bố, bên ngoài không có cách sẵn có nào để kiểm chứng, mà nạn nhân thì đang ở trong chiến tranh.

Vụ hack Viasat cho thấy đồng thời sức mạnh và giới hạn của tấn công mạng. Nhìn bằng lăng kính kỹ thuật và tác chiến, Nga đã chứng minh năng lực đánh sập hạ tầng dân sự tại sáu quốc gia bên kia biên giới, theo một chuỗi liên hoàn, với thời điểm chính xác trong phạm vi một giờ. Nhìn bằng lăng kính chiến lược, năng lực ấy không làm Kyiv sụp đổ nhanh chóng. Cùng một sự kiện vừa là bằng chứng về năng lực, vừa là thất bại trong việc đạt mục tiêu, và điều chúng ta đang làm lúc này chỉ là chọn gọi nó theo lăng kính nào. Chúng ta chưa có một câu trả lời đã ổn định.

Viasat là một công ty Mỹ. Mạng này không do chính phủ Ukraine xây dựng, cũng không thuộc sở hữu của quân đội Ukraine. Ngay cả trước chiến tranh, quân đội, chính phủ và dân thường Ukraine đã cùng dùng dịch vụ vệ tinh của công ty này, và các hộ gia đình châu Âu cũng dùng cùng dịch vụ đó. Nói cách khác, thông tin liên lạc quân sự của một quốc gia đã chạy trên một dịch vụ thương mại của một công ty nước ngoài.

Điều đáng lưu ý là cách hình dạng của vụ việc được biết đến. Mốc thời gian, sớm hơn lực lượng mặt đất một giờ, đến từ bài đưa tin của Patrick Howell O'Neill trên Technology Review, tạp chí do Massachusetts Institute of Technology xuất bản. Nhận định rằng vụ tấn công mạng là một cuộc tấn công được chuẩn bị theo nhiều tuyến đến từ Christian Vasquez và Elias Groll của CyberScoop, còn Matt Burgess của Wired và CyberPeace Institute gọi đó là một vụ tấn công vệ tinh bí ẩn đã gây thiệt hại cho cả những nạn nhân ngoài Ukraine. Điều tái dựng lại sự kiện không phải là hồ sơ vụ án của một điều tra viên, mà là các bài đưa tin của nhà báo và phân tích sau đó của các công ty an ninh. Tính chất của chứng cứ có được ngay từ đầu đã là như vậy.

Cũng cần giải thích tuyên bố chung ngày 10 May là loại công cụ gì. Thủ tục mà European Union, United States, United Kingdom và các nước Five Eyes khác dùng để nêu tên cơ quan tình báo quân sự Nga là bên đứng sau vụ tấn công được gọi là attribution trong an ninh mạng. Đó là một hành vi chính trị, trong đó nhiều nước cùng nói ra một cái tên để làm cho một sự kiện trở nên chắc hơn, chứ không phải phán quyết có tội của tòa án. Sau tuyên bố đó, ai bị đưa ra xét xử và hình phạt nào được áp dụng không xuất hiện trong các tài liệu công khai.

2. Các cuộc tấn công mạng và các đợt tấn công bằng tên lửa có diễn ra cùng nhau không?

Câu hỏi mà Viasat để lại đi thẳng vào một câu hỏi lớn hơn. Các cuộc tấn công mạng và các đợt tấn công bằng tên lửa của Nga có vận hành cùng nhau theo một lịch trình duy nhất không? Các hacker và pháo binh có đang nghe lệnh từ cùng một chỉ huy không?

Câu hỏi này quan trọng vì cách phản ứng của bên phòng thủ sẽ thay đổi theo câu trả lời. Nếu hai hoạt động này được phối hợp, một cảnh báo mạng cũng là một cảnh báo tên lửa, và khi máy chủ rung chuyển một cách bất thường, các đơn vị phòng không cũng phải căng mình theo. Nếu chúng không được phối hợp, đó là những cuộc chiến riêng rẽ vận hành theo nhịp riêng, và

từng cuộc chiến phải được chặn lại theo cách riêng.

Có một số trường hợp hai hoạt động này dường như chồng lên nhau. Viasat được tính là trường hợp đầu tiên. Một giờ trước khi lực lượng mặt đất vượt qua biên giới là thời điểm quá chính xác để gọi là trùng hợp, và chính độ chính xác ấy là lý do Bateman nhắc đến một 'mục đích quân sự rõ ràng'.

Tháp truyền hình Kyiv ngày 1 tháng 3 năm 2022 dẫn tới cùng một vấn đề. Báo cáo của CNA ghi rằng khi cơ sở này bị tên lửa đánh trúng, các cuộc tấn công mạng nhằm vào mạng lưới của các đài phát thanh truyền hình lớn cũng diễn ra song song. Hai cách cắt đứt phát sóng đã được dùng cùng nhau trong cùng một ngày. Một cách phá hủy tòa tháp, cách kia phá hỏng máy tính của đài phát sóng, và kết quả nhắm tới là như nhau: ngăn người dân Ukraine nghe thấy tiếng nói của chính phủ mình.

Cặp phương thức tương tự xuất hiện vào mùa đông. Sau khi các tiền tuyến đã cứng lại, Nga dùng các đòn tấn công tên lửa và hoạt động tấn công mạng cùng lúc để cắt hệ thống sưởi và điện của Ukraine, và mục tiêu là điều kiện sống còn của dân thường.

Một con số cho thấy quy mô của vấn đề. Theo một thống kê được trích dẫn trong cả báo cáo của CNA và Henry Jackson Society, từ khi cuộc xâm lược bắt đầu đến hết tháng 4 năm 2022, ít nhất sáu nhóm hacker riêng biệt có liên hệ với Nga đã thực hiện 237 chiến dịch mạng nhằm vào Ukraine. Các loại mã độc phá hủy mạng, như Whispergate và Foxblade, được triển khai hết lần này đến lần khác. Nghĩa là 237 chiến dịch chỉ trong hơn hai tháng, mỗi ngày ba hoặc bốn chiến dịch. Các cuộc tấn công mạng diễn ra hằng ngày; chúng chỉ không thu hút ánh mắt của thế giới.

Chính con số ấy cũng là cái bẫy trong cuộc tranh luận về phối hợp. Lịch trình trùng nhau và hai cuộc tấn công được phối hợp dưới cùng một chuỗi chỉ huy không phải là cùng một mệnh đề. Nếu các cuộc tấn công mạng xảy ra ba hoặc bốn lần mỗi ngày, còn các đợt tấn công bằng tên lửa diễn ra gần như mỗi ngày, thì việc một vụ hack cũng xảy ra ở đâu đó vào đúng ngày một quả tên lửa rơi xuống tự thân nó không có gì đáng ngạc nhiên. Chỉ xét theo xác suất ngẫu nhiên, khả năng hai sự kiện rơi vào cùng một ngày gần các mục tiêu tương tự không hề thấp.

Có một khoảng cách rất xa giữa việc chọn ra vài tổ hợp gây chú ý và việc chứng minh rằng các đơn vị mạng cùng các đơn vị tên lửa đã dùng chung một danh sách mục tiêu. Việc thứ nhất là thu thập trường hợp, việc thứ hai là chứng minh quan hệ nhân quả, và dù có bao nhiêu trường hợp đi nữa thì quan hệ nhân quả cũng không tự nó phát sinh.

Muốn khép lại khoảng cách đó, cần có tài liệu tác chiến của Nga hoặc tài liệu về chuỗi chỉ huy, tức giấy tờ cho thấy ai đã chỉ thị cho ai, vào lúc nào, làm việc gì. Hiện chưa có tài liệu nào như vậy được công khai, và cũng không có dấu hiệu nào cho thấy chúng sẽ được công khai.

Những giới hạn của hồ sơ công khai được giữ nguyên như vậy. Các báo cáo được dựa vào cho đến nay đều đến từ phía phòng thủ: các tổ chức phân tích phương Tây, các công ty Mỹ, chính

quyền Ukraine. Trong danh sách tài liệu công khai không xuất hiện tài liệu gốc nào trong đó Bộ Quốc phòng Nga hoặc các cơ quan tình báo của Nga giải thích phương pháp phối hợp của chính họ. Đây là cách xem một trận đấu từ một phía khán đài. Từ đó, ta có thể thấy bóng đã đi đâu, nhưng không biết huấn luyện viên đã gọi bài đánh nào.

Vì vậy, đối với câu hỏi liệu họ có hành động cùng nhau hay không, điều có thể nói chỉ dừng lại ở sự tương quan quan sát được từ bên ngoài. Không thể nói chắc về quan hệ nhân quả được truyền ra từ bên trong. Lời cảnh báo rằng phân tích sẽ chao đảo khi rút kết luận từ chứng cứ ban đầu chưa đầy đủ không chỉ đúng với tranh cãi Viasat, mà cũng đúng với tranh cãi về sự đồng bộ này.

Ngay cả khi không thể giải quyết dứt điểm câu hỏi về phối hợp, một sự thật vẫn chắc chắn: cuộc chiến này đã làm thay đổi bản chất của mục tiêu.

Trong chiến tranh truyền thống, cắt mạng liên lạc của đối phương có nghĩa là ném bom một tháp truyền dẫn hoặc cắt đứt một tuyến cáp. Việc đó đòi hỏi vũ khí phải chạm tới vấn đề bằng phương tiện vật lý. Máy bay ném bom phải cất cánh, tầm bắn của tên lửa phải đủ xa, và trên đường đi phải xuyên qua hệ thống phòng không. Phạm vi của chiến tranh được xác định bởi khoảng cách mà vũ khí có thể vươn tới.

AcidRain đã lan tới các tua-bin gió ở Đức. Không cần máy bay ném bom, không cần vượt qua biên giới, mà đi theo đường quản lý mạng của một công ty. Khái niệm về tầm với vì thế trở nên mờ đi. Một vũ khí nhắm vào Ukraine đã xuất hiện trong các gia đình ở Ba Lan và Hy Lạp, những quốc gia chưa từng đồng ý với cuộc tấn công và cũng chưa từng tham chiến. Vì vậy Liên minh châu Âu, Hoa Kỳ và Vương quốc Anh thấy cần phải ra một tuyên bố chung.

Bộ Chuyển đổi Số do Fedorov lãnh đạo phải vận hành một nhà nước trong điều kiện như vậy. Quyết định đưa dữ liệu chính phủ ra ngoài biên giới và quyết định khẩn cấp đưa các thiết bị đầu cuối internet vệ tinh vào trong nước đều là câu trả lời cho điều kiện đó. Vì sao phải vội, một sự kiện đã giải thích đủ: ngay trong ngày đầu tiên của cuộc xâm lược, một mạng thông tin vệ tinh đã bị xóa sổ.

Đối với một quốc gia từng tự hào về chính phủ điện tử, sự cảnh giác với an ninh mạng tăng lên sau sự cố này. Nói rằng một nhà nước được đặt vào trong điện thoại thông minh cũng có nghĩa là một nhà nước được đặt lên mạng, và thứ đã đặt lên mạng thì có thể bị xóa cùng với mạng đó.

Câu hỏi về phối hợp không chỉ nằm ở phía Nga. Nó cũng nằm ngang như vậy ở phía Ukraine. Ngay sau cuộc xâm lược, các hacker và công dân từ khắp thế giới đổ về 'IT Army of Ukraine' được tập hợp trên một kênh Telegram, và quy mô công khai đã được xác nhận là khoảng 150.000 người đăng ký Telegram. Số người đăng ký và số người thật sự tham gia tấn công là hai chuyện khác nhau, và về việc có bao nhiêu người đã tấn công hạ tầng số của Nga, hiện vẫn còn

quá sớm để kết luận từ hồ sơ công khai. Vì thế các nhận định chia rẽ quanh câu hỏi: đây là một đơn vị do nhà nước chỉ huy, hay là một nhóm do công dân tự hình thành.

Lập trường chính thức của chính phủ là việc này diễn ra trên cơ sở tự nguyện. Victor Zhora đã vạch rõ ranh giới: ông biết ơn các nhóm tình nguyện, nhưng hoạt động này hoàn toàn tự nguyện và nhà nước không điều phối. Fedorov cũng nói mạnh về quyền đạo đức được bảo vệ tính mạng công dân, trong khi công khai và nhiều lần phủ nhận nghi ngờ rằng nhà nước đã cho phép hoặc chỉ đạo hoạt động tấn công mạng nhằm vào các mục tiêu dân sự của Nga.

Những chứng cứ gián tiếp chỉ theo hướng ngược lại cũng rất rõ. IT Army khởi đầu bên dưới bề mặt khi doanh nhân công nghệ thông tin Yegor Aushev, theo yêu cầu của một quan chức cấp cao trong bộ quốc phòng, tập hợp một nghìn hacker, và Fedorov đưa ra lời kêu gọi công khai tham chiến trên kênh Telegram của chính ông vào ngày 26 February. Có hồ sơ cho thấy Ministry of Digital Transformation đã tuyển người cho hoạt động tấn công mạng dựa vào đám đông này, và một danh sách mục tiêu trải từ các cơ quan truyền thông Nga đến ngân hàng và cơ quan chính phủ đã được cập nhật đều đặn rồi chuyển xuống dưới. Bên trong tổ chức có 25 đến 30 'generals' được cho là đến từ các cơ quan tình báo và các bộ trong chính phủ, và dưới họ là các 'colonels' trực tiếp thực hiện những cuộc tấn công phá hoại trên thực tế. Một nhân vật từng hoạt động như hacker tình nguyện trước khi nhập ngũ vào lực lượng chính quy đã làm chứng rằng ngay khi đó đã có sự phối hợp với các cơ quan chính phủ.

Cuộc tranh cãi này không dừng ở lời nói. Luật quốc tế có hai tiêu chuẩn để gắn hành vi của dân sự với một nhà nước. Theo tiêu chuẩn kiểm soát hiệu quả, trách nhiệm chỉ phát sinh nếu chứng minh được không còn nghi ngờ rằng nhà nước đã thực thi quyền chỉ huy đầy đủ. Theo tiêu chuẩn kiểm soát tổng thể, trách nhiệm phát sinh nếu nhà nước chỉ cần tổ chức, điều phối và hỗ trợ. Ukraine có thể vượt qua tiêu chuẩn thứ nhất, nhưng không vượt qua được tiêu chuẩn thứ hai. Trên thang mười bậc do một báo cáo đưa ra, quan hệ này trong giai đoạn đầu của cuộc chiến nằm giữa bậc bốn, 'được nhà nước khuyến khích', và bậc sáu, 'được nhà nước điều phối'. Quốc hội Ukraine và Ministry of Digital Transformation đã soạn một dự luật để đưa các hacker này vào lực lượng chính quy như một lực lượng dự bị mạng; nếu luật đó được thông qua, địa vị sẽ tăng lên bậc mười, 'được tích hợp vào nhà nước', và toàn bộ hoạt động tấn công mạng của họ trở thành trách nhiệm của nhà nước.

3. Luận điểm thất bại và luận điểm tiêu hao kéo dài trong chiến tranh mạng của Nga

Trước khi chiến tranh bắt đầu, các chuyên gia an ninh mạng phương Tây phần lớn đều vẽ ra cùng một bức tranh, và bức tranh đó có cơ sở.

Từ lâu, Nga đã được đánh giá là xem Ukraine như một bãi thử cho chiến tranh mạng. Năm 2015 và 2016 xảy ra các vụ tấn công vào lưới điện của Ukraine. Giữa mùa đông lạnh giá, điện tắt

ở nhiều thành phố, và chỉ về sau người ta mới biết đó là một vụ hack. Năm 2017, mã độc NotPetya lan ra ngoài Ukraine tới 65 quốc gia. Đoạn mã nhắm vào Ukraine đã làm sập các hệ thống kế toán và hậu cần của nhiều công ty trên khắp thế giới.

Nhìn vào hồ sơ đó, các chuyên gia dự đoán một cú sốc ngang tầm cái gọi là 'cyber Pearl Harbor' sẽ xảy ra cùng lúc với cuộc xâm lược toàn diện. Đó là kịch bản trong đó các chức năng của một nhà nước ngừng hoạt động chỉ trong vài ngày. Bức tranh được hình dung là điện bị cắt, ngân hàng đình trệ, chính phủ không thể nói một lời nào với người dân của mình.

Nhưng sự tê liệt mà họ lo sợ, ở quy mô ấy, đã không xảy ra. Mùa xuân năm 2022, tuần báo Anh The Economist đưa tin về sự vắng mặt đáng chú ý của các cuộc tấn công mạng quy mô lớn nhằm vào Ukraine. Chuyên trang War on the Rocks đăng một bài phân tích chỉ ra thất bại của các chiến dịch mạng của Nga. Đánh giá khi đó là các cuộc tấn công mạng đã không thể cưỡng ép làm đổi hướng cuộc chiến. Vì vậy, 'luận điểm về thất bại của chiến tranh mạng Nga' bắt đầu đứng vững.

Điều gì bị quy trách nhiệm cho thất bại ấy? Nhà phân tích Justin Sherman nêu ra năm lý do khiến tác động của các chiến dịch mạng của Nga bị kìm lại: khó phối hợp giữa các miền tác chiến, hạn chế về nguồn lực, cạnh tranh giữa các cơ quan tình báo, ưu tiên chiến lược có chủ ý, và năng lực phòng thủ của Ukraine.

Trong số đó, yếu tố được nhiều phân tích đặt trọng lượng lớn nhất là cạnh tranh giữa các cơ quan tình báo. Năng lực mạng của Nga không tập trung trong một tổ chức duy nhất, mà phân tán ở nhiều cơ quan. Cơ quan tình báo quân sự được nêu tên đằng sau vụ tấn công Viasat chỉ là một trong số ấy. Cách đọc ở đây là sự cạnh tranh nội bộ giữa các cơ quan này về hạ tầng và thẩm quyền, cùng với việc thiếu một cơ chế phối hợp có thể đặt các chiến dịch của họ vào cùng một hướng, đã bào mòn chính năng lực của họ.

Yurii Shchyhol, người đứng đầu Cơ quan Nhà nước về Truyền thông Đặc biệt và Bảo vệ Thông tin của Ukraine, đưa ra một cách giải thích khác. Nga đã không ngờ Ukraine có thể trụ vững trước làn sóng tấn công mạng đầu tiên, và các kế hoạch của Nga cho tình huống đó không đủ. Nga tin chắc vào một chiến thắng nhanh và dứt khoát đến mức đã không tích trữ khối lượng năng lực mạng và các kế hoạch mà một cuộc chiến dài ngày sẽ cần.

Đó là một chẩn đoán có sức thuyết phục. Nhưng cần đặt nó cạnh sự thật rằng người nói là quan chức chịu trách nhiệm về phòng thủ mạng của chính phủ Ukraine. Những lời chỉ ra sự thiếu chuẩn bị của đối phương đồng thời cũng là những lời giải thích thành tích của tổ chức mình. Phía Nga giải thích tình hình ra sao nằm ngoài phạm vi các tài liệu công khai. Viết về thắng và bại dựa trên lời kể của một bên mà thiếu bên kia thì gần với việc phát thông cáo báo chí hơn là ghi chép lịch sử.

Nửa còn lại của luận điểm thất bại là phản ứng của Ukraine, cùng các công ty và chính phủ đứng sau nước này.

Các thiết bị AWS Snowball và sự hỗ trợ đám mây của Microsoft đã thấy ở Chương 2 cho thấy kết quả của chiến tranh mạng không chỉ do công nghệ tấn công quyết định. Sao lưu dữ liệu, lưu trữ ở nước ngoài và phát hiện mối đe dọa từ các đồng minh đã hạn chế những gì các cuộc tấn công của Nga đạt được.

Bên dưới sức chống chịu mạng của Ukraine là sự hỗ trợ từ chính phủ United States, các công ty American và United Kingdom. Nếu chỉ nói về sức chống chịu như một phẩm chất của riêng một quốc gia, ta sẽ xóa đi câu hỏi phẩm chất ấy đã đứng trên nguồn lực của ai. Khi đọc câu rằng nhà nước số của Fedorov không dừng lại ngay cả trong ngày đầu tiên của cuộc xâm lược, sự thật này phải được đặt bên cạnh nó để cán cân được cân bằng.

Khi luận điểm thất bại lan rộng, một phản biện nhanh chóng xuất hiện. Bài viết của Cattler và Black trên Foreign Affairs là đại diện cho phản biện ấy, với nhan đề 'The Myth of the Missing Cyberwar'. Lập luận diễn ra như sau: thứ vắng mặt không phải là các cuộc tấn công, mà là cảnh sụp đổ kiểu điện ảnh mà công chúng đã tưởng tượng. Các cuộc tấn công của Nga chưa bao giờ ngừng lại.

Bằng chứng nằm ở những con số đã thấy. Sáu nhóm và 237 chiến dịch chỉ trong hơn hai tháng. Vụ hack Viasat diễn ra một giờ trước cuộc xâm lược. Thiệt hại lan sang sáu quốc gia châu Âu. 5.800 tuabin gió ở Đức. Nhìn vào tất cả những điều đó rồi nói rằng không có tấn công mạng, theo lập luận phản bác, không phải là sự bất lực của Nga mà là thất bại của người quan sát.

Hai phe đang trả lời hai câu hỏi khác nhau. Luận điểm thất bại trả lời câu hỏi: "các cuộc tấn công mạng có làm thay đổi bên thắng trong cuộc chiến không?" Lập luận phản bác trả lời câu hỏi: "có các cuộc tấn công mạng không?" Hai câu trả lời lần lượt là không và có, và cả hai đều có thể đúng.

Điểm dung hòa mà các chuyên gia đi đến là như sau. Các chiến dịch mạng của Nga không thiếu khối lượng hoạt động ở cấp chiến thuật. Nếu chúng thất bại, thì thất bại nằm ở cấp chiến lược, tức cấp độ làm thay đổi bên thắng trong một cuộc chiến. Vũ khí mạng đã hoạt động bền bỉ, nhưng chúng không kết thúc được cuộc chiến.

Khi chiến thắng chớp nhoáng sụp đổ và chiến tuyến đông cứng lại, các chiến dịch mạng của Nga cũng đổi tính chất. Clint Watts phân tích rằng các chiến dịch gây ảnh hưởng và chiến dịch mạng của Nga đang thích nghi với một cuộc chiến dài và khoét sâu vào 'sự mệt mỏi vì chiến tranh' của phương Tây. Sự mệt mỏi vì chiến tranh là trạng thái trong đó công chúng ở các nước ủng hộ bắt đầu chán nản và nói rằng đã đủ rồi. Đó là con đường khiến sự hỗ trợ bị cắt đứt, không phải vì vũ khí cạn kiệt, mà vì ý chí đã hao mòn.

Ở giai đoạn này, mục tiêu chuyển từ sở chỉ huy ngoài tiền tuyến sang tâm trí ở hậu phương. Báo cáo của CNA ghi nhận rằng Nga dồn sức cho các chiến dịch thông tin nhằm khoét sâu chia rẽ trong xã hội phương Tây. Những luận điệu bị thao túng lan rộng, rằng dòng người tị nạn Ukraine đang làm giảm mức sống của người châu Âu, rồi tiếp đó là tuyên truyền bào mòn lòng tin quốc tế đối với Ukraine. Cùng lúc, mục tiêu của tấn công mạng mở rộng sang lưới điện và hậu cần. Tên lửa và tấn công mạng được dùng cùng nhau để cắt sưởi ấm và điện trong mùa đông, với kết quả nhắm tới là làm dân thường kiệt sức.

Đây là 'luận đề tiêu hao kéo dài'. Nó đánh giá lại chiến tranh mạng như một kỹ thuật ít nhằm tung ra một đòn quyết định duy nhất, mà nhằm mài mòn hạ tầng và sự kiên nhẫn của đối phương theo thời gian, không phải sự sụp đổ kịch tính mà là chảy máu dai dẳng.

Đặt hai diễn ngôn này chồng lên nhau, bức tranh hiện ra như sau. Các cuộc tấn công mạng không kịch tính như người ta từng dự đoán, nhưng chúng cũng không biến mất. Chúng không kết thúc chiến tranh, nhưng được dùng để kéo dài chiến tranh.

Bài học mà bức tranh này đem lại cho bên phòng thủ lại quay về tính dự phòng. Nếu một mạng vệ tinh bị xóa sổ nhưng vẫn còn một đường khác, chỉ huy vẫn tiếp tục. Dữ liệu đặt trên một máy chủ duy nhất trong biên giới sẽ biến mất cùng một quả tên lửa; dữ liệu được phân tán trên các đám mây của nhiều quốc gia thì không. Tính dự phòng mà Victor Zhora nói đến là một nguyên tắc thiết kế trước khi trở thành lời giải thích sau sự việc.

Kết luận này cũng giải thích vì sao sau đó Fedorov và bộ của ông đặt nguồn lực vào đâu. Ngay trong năm 2022, điều đã rõ là phòng thủ và phản công riêng trong không gian mạng không thể đẩy lùi lực lượng mặt đất của Nga. Kết cục của cuộc chiến được quyết định trong chiến hào, trên các tuyến đường, trên bầu trời, và giữa những cỗ máy rẻ tiền đang bay ở đó.

Nếu được hỏi chiến tranh mạng đã thay đổi điều gì, có thể trả lời như sau. Chiến tranh mạng không thay đổi cách một cuộc chiến kết thúc. Nó thay đổi phạm vi mà chiến tranh có thể vươn tới, và thay đổi những gì một nhà nước phải phân tán từ trước, theo nhiều lớp, nếu muốn sống sót.

Những câu hỏi còn lại vẫn để ngỏ. Vụ hack Viasat là một đòn lớn đến mức nào? Các hacker và pháo binh có đang đọc cùng một mệnh lệnh hay không? Chiến tranh mạng của Nga là một thất bại, hay là một kiểu thành công khác vẫn đang tiếp diễn? Với ba câu hỏi này, thứ chúng ta có là bằng chứng quan sát được từ phía phòng thủ, các tuyên bố của quan chức mâu thuẫn với nhau, và những báo cáo tự nói rằng chúng chưa đầy đủ. Biết chính xác điều mình chưa biết giúp hiểu cuộc chiến này hơn là giả vờ đã biết câu trả lời.

Nguồn gốc của con số 237 cần được nói rõ. Con số tổng hợp này đến từ một báo cáo của Microsoft. Cũng chính công ty đó là bên cung cấp dịch vụ đám mây cho chính phủ Ukraine. Clint Watts, người phân tích rằng các chiến dịch mạng của Nga đang thích nghi với một cuộc chiến

dài và khoét sâu vào sự mệt mỏi chiến tranh ở phương Tây, cũng thuộc Microsoft. Việc bên thống kê và bên phòng thủ là một không làm cho con số ấy sai. Nhưng sẽ trung thực hơn nếu ghi kèm rằng hồ sơ mạng của cuộc chiến này phần lớn được tạo ra trong tay các công ty đã tham gia phòng thủ.

Giọng điệu mà luận điểm về thất bại lan ra vẫn còn hiện rõ trong các tiêu đề. The Economist nói đến sự vắng bóng dễ thấy của những cuộc tấn công quy mô lớn, còn bài viết trên War on the Rocks mang nhan đề 'Why Russia's Cyber Dogs Have Mostly Failed to Bark'. Bài phân tích của Justin Sherman mang nhan đề 'Untangling Russia's Cyber Matryoshka'. Matryoshka là loại búp bê gỗ Nga, bên trong có những con búp bê nhỏ hơn lồng vào nhau, lớp này trong lớp khác. Nhan đề ấy hàm ý rằng năng lực mạng của Nga không phải là một khối duy nhất, mà bị chia thành nhiều tầng.

Tên của các tầng ấy là cơ quan tình báo quân đội (GRU), cơ quan tình báo đối ngoại (SVR), và cơ quan an ninh liên bang (FSB). Đơn vị được nêu đằng sau vụ tấn công Viasat chỉ là một trong số đó. Sự cạnh tranh nội bộ giữa các cơ quan này về hạ tầng mạng và thẩm quyền, cùng với việc thiếu phối hợp để các chiến dịch của họ đi cùng một hướng, đã tự cắt giảm năng lực của chính họ. Đó là chẩn đoán trong nhiều bài phân tích.

Ở phía Ukraine, điều ngược lại đã xảy ra. Sự hỗ trợ của Mỹ và Anh không vội vã đổ vào sau khi cuộc xâm lược bắt đầu; nó đã có sẵn ngay trước thềm chiến tranh. Khả năng chống chịu là cái tên được đặt cho một kết quả, và trong kết quả ấy có trộn lẫn nguồn lực của người khác đã đến từ trước.

Chương 6. Từ gọi vốn cộng đồng đến đội quân drone

1. Mạch nối biến các khoản quyên góp cho UNITED24 thành drone

Tháng 6 năm 2022, trên sân khấu Cannes Lions International Festival of Creativity tại Cannes, Pháp, nền tảng gây quỹ UNITED24 của chính phủ Ukraine được giới thiệu. Một liên hoan nơi những người sống bằng nghề quảng cáo và marketing trao giải cho nhau, và ngay tại đó một quỹ quốc gia của một nước đang có chiến tranh được công bố: bản thân sự kết hợp ấy đã lạ. Hai tháng sau, tại Ukraine Recovery Conference ở Lugano, Thụy Sĩ, UNITED24 trình bày bản báo cáo đầu tiên. Số tiền quyên góp trong hai tháng đầu của nền tảng đã vượt 75 triệu dollars. Cũng tại địa điểm ấy, nền tảng kêu gọi người tham gia Army of Drones (Армія дронів). Trong ba ngày, số tiền huy động đạt khoảng 200 triệu hryvnias.

Thu tiền quyên góp và dùng số tiền đó để mua vũ khí rồi đưa đến các đơn vị là hai công việc khác nhau. Việc thứ hai khó hơn việc thứ nhất rất nhiều, nhưng điều đó không hề được viết trong các thông báo của mùa hè năm ấy.

Ở bất kỳ quốc gia nào trên thế giới, tiền mua vũ khí đều lấy từ ngân sách quốc phòng. Quốc hội phê chuẩn ngân sách, một cơ quan mua sắm mở thầu, hợp đồng được ký, hàng hóa đi qua kho rồi đến đơn vị. Tuyến đường này chậm. Nó chậm là có lý do. Mua vũ khí bằng tiền thuế phải đi kèm giám sát và hồ sơ. Chỉ khi có hồ sơ ai đã mua gì, với giá bao nhiêu, người ta mới có thể đặt câu hỏi về sau; và chỉ khi có thể đặt câu hỏi, tiền mới ngừng rò rỉ. Mua sắm chậm vì sự chậm ấy đã được thiết kế vào nó ngay từ đầu.

Ukraine năm 2022 không ở trong tình thế có thể chịu được sự chậm chạp được thiết kế như vậy. Các đơn vị ngoài tiền tuyến cần những máy bay không người lái có thể bay ngay trong ngày, còn quy trình thông thường sẽ đưa chúng tới sau nhiều tháng. Mykhailo Fedorov, Bộ trưởng Chuyển đổi số, đã xây dựng một kênh riêng nối các khoản thanh toán bằng thẻ của công dân khắp thế giới với việc mua máy bay không người lái cho quân đội Ukraine. Mạch này không xóa bỏ tuyến mua sắm của Bộ Quốc phòng. Nó là một đường thứ hai đặt song song với tuyến đó, và chênh lệch tốc độ giữa hai đường sẽ định hình lại địa hình của ngành công nghiệp quốc phòng Ukraine trong những năm sau đó.

Các khoản quyên góp bắt đầu trên điện thoại thông minh. Ngay từ những ngày đầu của cuộc chiến, Fedorov đã đăng địa chỉ ví tiền mã hóa của chính phủ lên mạng xã hội và kêu gọi đóng góp. Ông nhìn phương thức này vừa là cách gây quỹ, vừa là cách giữ sự chú ý của thế giới. Phán đoán của ông là ngay cả một khoản quyên góp nhỏ cũng tạo ra một mối liên hệ giữa một cá nhân ở đâu đó trên thế giới với Ukraine, và giữ cuộc chiến nằm trong màn hình của mọi người. Một người cho năm đô la sau đó sẽ tiếp tục tìm tin tức từ Ukraine. Fedorov tin rằng gây quỹ có thể cùng lúc gom tiền và gom sự chú ý của thế giới.

Phán đoán này đi vào Diia, ứng dụng hành chính nhà nước. Diia bổ sung các chức năng quyên góp cho UNITED24 và mua trái phiếu chiến tranh. Trên cùng màn hình nơi họ vẫn xem thẻ căn cước và giấy phép lái xe, công dân giờ đây có thể đóng thêm vào ngân sách quốc phòng. Các báo cáo nghiên cứu mô tả sự kết hợp này như việc một ứng dụng hành chính đổi tính chất thành một công cụ fintech để tài trợ chiến tranh. Trong ba tháng đầu sau khi cuộc xâm lược bắt đầu, hơn 166 triệu đô la đã được huy động cho nhu cầu quân sự và nhân đạo. Các hạng mục hỗ trợ có thể thực hiện qua Diia bao gồm gây quỹ cho máy bay không người lái, và hàng chục triệu hryvnia đã đi theo tuyến này tới quân đội Ukraine và Army of Drones.

Có ngân sách không có nghĩa là máy bay không người lái lập tức được triển khai ra tiền tuyến. Ukraine năm 2022 có các công ty nhỏ và xưởng sản xuất rải khắp đất nước có thể chế tạo máy bay không người lái, nhưng phần lớn chưa từng giao bất cứ thứ gì cho quân đội. Muốn cung cấp cho quân đội, bạn phải vượt qua các bài kiểm tra của Bộ Quốc phòng và nhận một mã chính thức. Mã là số đăng ký đưa một mặt hàng vào danh mục tiếp tế của quân đội. Không có số đó, dù một món đồ bay tốt đến đâu, quân đội cũng không thể trả tiền cho nó. Để có được số này, bạn cần báo cáo thử nghiệm và tài liệu kỹ thuật, và cần một người từng viết những tài liệu như vậy. Một công ty có hai mươi nhân viên không có người như thế. Một kỹ thuật viên từng tạo hình cánh quạt trong nhà kho không thể bỗng nhiên bắt đầu viết hồ sơ hành chính quân sự.

Dự án Army of Drones tập trung vào việc rút ngắn độ trễ giữa mua sắm, thử nghiệm và triển khai. Chính phủ Ukraine đã nới lỏng đáng kể mức trần biên lợi nhuận đối với các nhà sản xuất drone thông qua "Nghị định số 256". Các báo cáo phân tích ghi nhận rằng dự án Army of Drones được lập ra ngay sau đó. Trần biên lợi nhuận là mức giới hạn lợi nhuận mà một công ty được giữ lại khi bán hàng cho nhà nước. Nếu mức trần quá thấp, công ty càng sản xuất càng lỗ, và không ai bước vào một thị trường nơi họ mất tiền. Mục tiêu của dự án là dùng số tiền huy động qua UNITED24 để kéo các công ty mới vào thị trường và đưa họ vào chuỗi cung ứng drone cho quân đội. Dự án không dừng ở việc mua sản phẩm hoàn chỉnh. Nó cắt bớt các bước thử nghiệm và giấy tờ chứng nhận chất lượng, đồng thời bố trí nhân sự chuyên trách giúp các doanh nhân vượt qua các bài kiểm tra. Khi một nhà sản xuất nhận được mã của Bộ Quốc phòng, Army of Drones dùng tiền từ UNITED24 để trả trực tiếp chi phí sản xuất cho những drone sẽ được chuyển tới quân đội Ukraine.

Chính phủ trao cho các công ty vốn, cơ hội thử nghiệm và một kênh mua sắm. Chính phủ viết lại luật chơi để họ có thể có lãi, đẩy hồ sơ giấy tờ giúp họ, và mua những sản phẩm đầu tiên của họ. Trong thế giới startup, vai trò này được gọi là accelerator: một tổ chức gắn tiền, lời khuyên và khách hàng đầu tiên với một công ty mới ra đời cùng một lúc. Nền tảng gây quỹ trở thành cả một định chế hỗ trợ các doanh nghiệp quốc phòng non trẻ lẫn người mua đầu tiên của họ. Cách làm này về sau dẫn tới cụm công nghệ quốc phòng có tên Brave1. Các khoản quyên góp đi qua nới lỏng quy định và hỗ trợ giấy tờ, rồi chảy vào chi phí sản xuất của các công ty mới.

Ngày 30 tháng 10 năm 2022, Fedorov thông báo rằng ông sẽ tăng cường Army of Drones bằng các drone tấn công do Ukraine sản xuất, và các thỏa thuận hợp tác đã được ký với bốn công ty. Đây là thông báo của Bộ Chuyển đổi Số, và trọng tâm của nó nằm ở cụm từ "do Ukraine sản xuất". Đó là một tuyên bố về hướng đi: một quốc gia từng dựa vào hàng hóa mua từ nước ngoài sẽ chuyển sang thành một quốc gia mua những gì chính các công ty của mình làm ra. Một tuyến cung ứng dựa vào nhập khẩu bị treo trên quyết định của người khác. Chỉ một hạn chế xuất khẩu, chỉ một thay đổi trong chính sách của nhà sản xuất, cũng có thể khiến tiền tuyến mất đi đôi mắt. Dù vậy, thông báo không cho biết bốn hợp đồng đó tạo ra bao nhiêu máy bay. Đơn giá hợp đồng cũng không được công bố. Điều thông báo xác nhận chỉ dừng ở hướng đi của dự án; kết quả thực tế vẫn chưa có câu trả lời.

Mạch vận hành này không thể được đọc như lời tự khen của chính phủ Ukraine. Phân tích từ bên ngoài chính phủ xác nhận cùng một chức năng ấy. Một báo cáo nghiên cứu chính sách đánh giá rằng hệ thống điểm của Bộ Chuyển đổi Số và UNITED24 đã tạo ra một kênh mua sắm và phát triển bền vững. Phía sau đó, báo cáo nhìn thấy hoạt động mua sắm của chính phủ bị bộ máy hành chính làm chậm lại và năng lực ở tiền tuyến còn thiếu. Đây là một cấu trúc trong đó một nền tảng gây quỹ do chính phủ tạo ra lấp vào phần mà chính phủ không thể giao đúng lúc. Viết thành một câu thì nghe kỳ lạ, nhưng ở tiền tuyến, đó là một câu trả lời có thể cầm được trong tay.

Quy mô gây quỹ từ công dân cũng không nhỏ. Theo một phân tích của Forbes, các khoản quyên góp cho 50 tổ chức từ thiện hàng đầu cộng với gây quỹ công khai tương đương 2 đến 2,5 phần trăm tổng sản phẩm quốc nội của Ukraine trong năm 2023. Tổng sản phẩm quốc nội là tổng lượng của cải mà một quốc gia tạo ra trong một năm. Điều đó có nghĩa là khoảng một phần năm mươi của con số ấy đã chảy vào quốc phòng dưới danh nghĩa đóng góp tự nguyện của công dân. Khi một lượng tiền ở quy mô này di chuyển bên ngoài quá trình thảo luận ngân sách, người đứng tại các nút giao mà dòng tiền đi qua nắm trong tay một thứ quyền lực chưa từng được bỏ phiếu tại quốc hội.

Nhưng hồ sơ chi tiết về cách các khoản tiền được dùng đã không được công bố đầy đủ ngay từ đầu. Số tiền huy động được thì được công khai. Bao nhiêu tiền đi vào mẫu thiết bị nào của công ty nào thì không. Đơn giá hợp đồng có phù hợp hay không, và vì sao các công ty bị loại không được chọn, cũng vẫn chưa có câu trả lời. Không thể tìm được tài liệu kiểm toán độc lập xác nhận những điều này. Các con số đã công bố, phần lớn, là các giá trị do UNITED24, Bộ Chuyển đổi số và Bộ Quốc phòng công bố. Vẫn còn đó một cấu trúc trong đó chính phủ đã xây dựng hệ thống cũng là bên đánh giá kết quả của hệ thống ấy.

Bộ Chuyển đổi số đã xây dựng một kênh nối các khoản quyên góp với việc mua drone. Hai câu nói từ năm 2022 ấy trở thành đoạn đường đầu tiên mà, vài năm sau, sẽ đưa Fedorov vào tòa nhà Bộ Quốc phòng.

Fedorov trước đó đã kéo nguồn lực bên ngoài vào theo cách tương tự trong lĩnh vực thông tin liên lạc. Vào tháng 2 năm 2022, ngay trước cuộc xâm lược, tin tặc Nga đã tấn công mạng KA-SAT của công ty Mỹ Viasat. Hàng nghìn modem liên lạc vệ tinh mà quân đội và chính phủ Ukraine sử dụng bị vô hiệu hóa. Một số báo cáo và tuyên bố chính thức cho rằng vụ tấn công đã gây ra tổn thất liên lạc lớn trong mạng chỉ huy và kiểm soát, dù mức độ tác động của nó được đánh giá khác nhau trong các tài liệu. Ngày 26 tháng 2, Fedorov đề nghị Elon Musk cung cấp thiết bị đầu cuối Starlink trên X. Câu trả lời đến trong chưa đầy mười hai giờ. Hai ngày sau, lô hàng đầu tiên tới nơi. Cách kéo nguồn lực từ bên ngoài chính phủ thông qua mạng xã hội thay vì qua một chuỗi phê duyệt, đến lúc đó, đã qua một lần thử nghiệm. Bốn tháng sau, việc UNITED24 xuất hiện trên sân khấu tại Cannes chính là phương pháp ấy được chuyển sang lĩnh vực tiền bạc.

Khi dựa vào dịch vụ của một công ty tư nhân, quyết định của chính công ty đó cũng có thể cắt đứt dịch vụ. Khi quân đội Ukraine tiến hành một chiến dịch bằng tàu mặt nước không người lái ở vùng biển ngoài khơi Sevastopol, kết nối Starlink đã không hoạt động. Trong các tài liệu, có điểm khác nhau: liệu một dịch vụ vốn đã được bật bị chặn, hay Musk đã từ chối yêu cầu của Ukraine về việc mở rộng vùng phủ sóng. Điều được xác nhận là chiến dịch của các tàu không người lái bị mất liên lạc đã thất bại, và phạm vi sử dụng một mạng thông tin liên lạc lớn đã do SpaceX, một công ty, quyết định. Chứng cứ và giới hạn của cả hai cách giải thích được đặt cạnh nhau trong Chương 4.

Các khoản quyên góp đi qua UNITED24 được dùng để mua sắm drone cùng với ngân sách nhà nước. Đây là một trong ba nguồn mà Ukraine đã dùng để tài trợ cho việc mua drone từ năm 2014. Tiền từ các quỹ tư nhân lớn như Come Back Alive và Serhiy Prytula Foundation cũng chảy theo cùng hướng đó. Điều này có nghĩa là một phần không nhỏ số tiền chống đỡ quốc phòng phụ thuộc vào quyết định của các nhà tài trợ, chứ không phải vào quá trình thảo luận ngân sách. Kế hoạch cho tình huống các khoản quyên góp giảm xuống là gì, trong các tài liệu công khai đã thu thập được, hồ sơ công khai dừng lại ở đây.

2. Một dự án quốc gia gắn kết đào tạo phi công, sửa chữa và thay thế

Đưa một chiếc drone ra tiền tuyến không giống như gửi một kiện hàng. Drone phải có người điều khiển, phải được sửa khi hỏng, và phải được thay bằng chiếc mới khi không thể sửa được nữa. Nếu thiếu dù chỉ một trong ba việc này, hai việc còn lại cũng sụp đổ. Một chiếc drone không có phi công chỉ là một chiếc hộp trong nhà kho. Một đơn vị không có nhân sự sửa chữa sẽ cạn khung thân bay trong vòng một tháng. Khi việc thay thế đến muộn, một đơn vị càng chiến đấu giỏi thì càng sớm rơi vào cảnh tay trắng, vì dùng càng nhiều thì mất càng nhiều. Những gì Ukraine xây dựng sau năm 2022 không dừng lại ở một chương trình mua drone; nó phát triển thành một dự án quốc gia gắn đào tạo, sửa chữa và thay thế thành một hệ thống.

Việc huấn luyện phi công trong giai đoạn đầu của cuộc chiến nằm trong tay các tình nguyện viên và các trường dạy máy bay không người lái tư nhân. Những người từng bay drone như

một thú chơi thuê nhà kho, mở lớp, dạy những người hàng xóm sắp nhập ngũ cách cầm bộ điều khiển. Việc nhà nước làm là đưa nguồn năng lượng dân sự ấy vào hệ thống nhân sự của quân đội. Bộ Quốc phòng Ukraine lập ra một thủ tục để chính thức chứng nhận các tổ chức phi chính phủ dân sự và các trường tư nhân, rồi chứng nhận hơn 30 trường đào tạo phi công drone. Người tốt nghiệp các trường được chứng nhận đủ điều kiện nhận trình độ "Military Occupational Specialty Number 216: External Crew Member of Unmanned Aerial Vehicles."

Mã chuyên môn nghề nghiệp là thẻ số mà quân đội dùng để phân loại con người. Chỉ khi có một con số, một người mới tồn tại với tư cách "phi công drone" trong hồ sơ nhân sự của quân đội. Chỉ khi có một con số, anh ta mới được phân vào vị trí ấy; và khi vị trí ấy trống, nó được lấp bằng một người có cùng con số. Không có con số, dù bay giỏi đến đâu, trên giấy tờ anh ta vẫn là lính bộ binh; nếu anh ta tử trận, quân số bộ binh giảm đi một người, chứ không ghi nhận là mất một phi công. Những tổn thất không được đếm cũng không lọt vào kế hoạch bổ sung quân. Nhà nước chứng nhận các trường drone dân sự và gắn cho chúng một con số. Một kỹ năng học từ thú chơi bắt đầu được công nhận là chuyên môn quân sự. Sự thay đổi này về sau dẫn tới việc thành lập Unmanned Systems Forces.

Tên của các trường được chứng nhận tự chúng đã là một tấm bản đồ về địa hình của hệ sinh thái này. Borvibiter và Kruk là các trường được chứng nhận, giảng dạy các chuyên môn quân sự của Unmanned Systems Forces. Borvibiter chia khóa học theo loại máy bay: multirotor, fixed-wing, FPV multirotor. FPV nghĩa là "first-person view," một phương pháp trong đó phi công nhìn luồng hình ảnh từ camera gắn trên máy bay qua kính đeo và bay như thể đang ngồi bên trong nó. Killhouse Academy dạy dân thường và binh sĩ cách vận hành thực tế drone FPV. ProFPV UA Drone mở các khóa về cách điều khiển những khung máy bay thương mại như DJI Mavic và Autel EVO trong chiến đấu. UA Drone School duy trì một khóa chuyên sâu bốn ngày cho các đơn vị phải đưa người ra mặt trận gấp.

Các cơ sở đào tạo dân sự, trong đó có những trường này, nói rằng họ đã đào tạo hơn 250.000 người kể từ năm 2022. Nội dung giảng dạy gồm lái FPV, bảo trì, lập kế hoạch nhiệm vụ và tấn công tầm sâu. Con số 250.000 này là số do chính các cơ sở đào tạo cộng lại và công bố. Có bao nhiêu người tốt nghiệp thật sự cầm bộ điều khiển ở tiền tuyến, hồ sơ công khai dừng lại ở đây. Một khóa bốn ngày và một khóa kéo dài vài tuần có được tính như cùng một lần "hoàn thành" hay không cũng chưa có câu trả lời. Cũng không tìm thấy tài liệu đánh giá bên ngoài nào so sánh chất lượng đào tạo giữa các trường. Đọc nó như một chỉ dấu về quy mô thì chính xác hơn là xem như bằng chứng thành tích: nó cho thấy đất nước này đã đẩy bao nhiêu người vào công việc này.

Điều đó cũng không có nghĩa là việc huấn luyện không tốn tiền. Hãy xét trường hợp của một nhà sản xuất hàng đầu nước ngoài. Huấn luyện bốn phi công cho drone tình báo, giám sát và trinh sát tốn khoảng 30.000 euro. Thiết bị mà họ sẽ dùng tốn khoảng 100.000 euro. Tình báo,

giám sát và trinh sát là tên gọi chung cho các nhiệm vụ tìm kiếm, theo dõi và thu thập hiểu biết về đối phương. Vì trong những nhiệm vụ này không có thứ gì phát nổ, chúng hiếm khi xuất hiện trên bản tin, nhưng nếu thiếu chúng thì câu hỏi đánh vào đâu sẽ không có câu trả lời. Phép tính ở đây là đưa bốn người vào vị trí đó tốn 130.000 euro, và cụm từ "drone giá rẻ" đã bắt đầu trượt khỏi thực tế khi đặt trước chi phí huấn luyện và thiết bị này.

Sửa chữa còn khó hơn. Drone trên chiến trường bị bắn hạ, rơi, hoặc mất điều khiển vì gây nhiễu điện tử. Ngay cả những khung máy bay quay về được cũng cần thay cánh quạt, camera và pin trước khi có thể bay tiếp. Nếu nói theo ngôn ngữ ô tô, chuyện này giống như ngày nào cũng đâm xe và ngày nào cũng phải vào xưởng. Thực tế không hề trơn tru. Vì dịch vụ hậu mãi của các nhà sản xuất còn thiếu, thành viên các đơn vị chiến đấu phải tự lập đội để xử lý việc cải tiến, sửa chữa và nâng hiệu năng thiết bị. Các phi công drone ở tiền tuyến nhận khoản phụ cấp khoảng 3.000 đô la mỗi tháng. Có hồ sơ cho thấy họ đã tự bỏ tiền túi từ 5 đến 30 phần trăm khoản đó để sửa chữa và nâng cấp thiết bị.

Đã có những trường hợp binh sĩ dùng tiền riêng để sửa drone do nhà nước cấp. Gánh nặng ở mặt đất này phải được nhìn cùng với kết quả gây quỹ quy mô lớn. Ở đầu xa của chính vòng tuần hoàn nơi các khoản quyên góp từ khắp thế giới lấp đầy 200 triệu hryvnia trong ba ngày, một phi công đang tự quẹt thẻ để mua linh kiện. Hoạt động mua sắm trở nên nhanh hơn, nhưng điều đó không có nghĩa là sự hỗ trợ cần thiết đã đến được với từng binh sĩ.

Nhà nước phản ứng bằng cách đưa sửa chữa vào chương trình huấn luyện. Prometheus, một đơn vị Ukraine cung cấp các khóa học trực tuyến mở, đã mở khóa học mang tên "FPV for the People", dạy lắp ráp và bảo trì. Kyiv Drone Pilot vận hành một khóa kỹ thuật bao gồm cả kỹ năng điều khiển lẫn bảo trì. Dronarnia cung cấp đào tạo thực hành chuyên về lắp ráp, bảo trì và sửa chữa drone tấn công chiến thuật cùng sản xuất lô nhỏ. Ở tiền tuyến, phi công và thợ máy thường là cùng một người. Người lính phóng khung máy bay vào buổi sáng cầm mỏ hàn vào buổi tối. Đó là lý do hướng dẫn điều khiển và bảo trì được đưa vào cùng một chương trình.

Cơ chế xử lý việc thay thế là "Army of Drones Bonus", biến đoạn phim tấn công thành điểm và cho phép các đơn vị dùng số điểm đó để chọn loại drone họ cần. Cách chấm điểm và quy trình xác minh của hệ thống được trình bày ở Chương 10. Trong chương này, chúng ta nhìn vào việc quyền cấp phát đã dịch chuyển từ kho trung tâm về phía các lữ đoàn và đơn vị tuyến đầu.

Trong một quy trình mua sắm nhanh, khâu kiểm tra và các bước quy trách nhiệm có thể bị đẩy về phía sau. Việc phân phối thiết bị bằng điểm cũng có nghĩa là những nhiệm vụ dễ tạo điểm sẽ có lợi thế hơn những nhiệm vụ khó tạo điểm. Cách tính cho trinh sát, tiếp vận thông tin liên lạc, rà phá mìn và cứu hộ binh sĩ phe mình, tức những nhiệm vụ không có vụ nổ nào, chưa được công bố. Thẩm quyền và thủ tục đặt hệ số: hồ sơ công khai dừng ở đây. Ai lọc bỏ phần thổi phồng trong báo cáo thành tích cũng vẫn chưa có câu trả lời. Các tài liệu độc lập trả lời những câu hỏi này: trong phạm vi hồ sơ công khai đã thu thập, hồ sơ công khai dừng ở đây. Không có

căn cứ để nói rằng những người thiết kế hệ thống không biết vấn đề này, và cũng không có căn cứ để nói rằng họ đã giải quyết nó; chỉ còn các câu hỏi vẫn để ngỏ.

Cần nhìn rõ ai là người thật sự vận hành mạng lưới huấn luyện này. Phần lớn trong hơn ba mươi trường được chứng nhận không phải là cơ quan nhà nước, mà là các tổ chức phi chính phủ dân sự và trường tư. Nhà nước không tự xây trường mới. Nhà nước chứng nhận các trường tư vốn đã hoạt động. Việc giảng dạy thực tế do các tổ chức ngoài chính phủ đảm nhận. Nguồn kinh phí vận hành của các trường đến từ đâu: hồ sơ công khai dừng ở đây. Ai đặt ra tiêu chuẩn giảng viên và theo chuẩn nào cũng vẫn chưa có câu trả lời. Tiêu chí thu hồi chứng nhận cũng không tìm thấy trong các tài liệu công khai đã được công bố.

Hồ sơ cho thấy các đơn vị tự lập nhóm để cải tiến, sửa chữa và nâng cao hiệu năng cũng có nghĩa là các đơn vị chiến đấu đã kiêm luôn vai trò những xưởng nhỏ. Đây là trạng thái trong đó trách nhiệm hậu mãi lẽ ra thuộc về công ty sản xuất vũ khí đã được chuyển sang người sử dụng nó. Còn khoản 5 đến 30 phần trăm bị trích từ phụ cấp của binh sĩ được ghi vào mục nào trong thống kê chi tiêu quốc phòng của quốc gia, hoặc có được ghi hay không, thì không có tài liệu nào trong phạm vi thu được cho chúng ta biết.

Khi thẩm quyền thay thế được đẩy xuống dưới, chính các bên mua cũng trở nên đông đảo. Từ năm 2024, việc thực hiện ngân sách của chính quyền địa phương và việc các lữ đoàn mua trực tiếp đã được cho phép. Hàng hóa đến nhanh. Nhưng thủ tục tập hợp vào một nơi để so sánh ai đã mua gì, với giá nào: hồ sơ công khai dừng lại ở đây. Phương pháp kiểm toán để kiểm tra hồ sơ mua sắm của các lữ đoàn và chính quyền địa phương cũng không tìm thấy trong các tài liệu công khai đã được công bố. Khi mạch vận hành nhanh hơn, số cửa sổ để nhìn vào mạch đó lẽ ra cũng phải nhiều hơn, nhưng những cửa sổ ấy ở đâu thì vẫn chưa thấy rõ.

3. Huyền thoại về máy bay không người lái giá rẻ và thực tế của sản xuất, đạn dược và tác chiến điện tử

Các bài viết về cuộc chiến máy bay không người lái ở Ukraine thường ưa dùng một phép tương phản: một máy bay không người lái cảm tử giá vài trăm đô la phá hủy một xe tăng trị giá hàng triệu đô la. Những con số rất sắc nét, và bức tranh ấy đem lại cảm giác thỏa mãn. Phép tương phản này chứa một mảnh sự thật, nhưng nếu chỉ nhìn vào mảnh ấy, ta sẽ đọc ngược nền kinh tế của cuộc chiến.

Hãy nhìn vào chi phí huấn luyện và gánh nặng tự bỏ tiền của người lính, ta sẽ thấy những chi phí còn nằm lại trên mặt đất. Đưa bốn phi công vào công việc tình báo, giám sát và trinh sát tốn 130,000 euro cho huấn luyện và thiết bị. Những phi công được dựng lên theo cách đó lại phải bỏ một phần phụ cấp của mình để duy trì thiết bị. Không khoản nào trong số này xuất hiện trên nhãn giá của thân máy bay. Không phải máy bay không người lái rẻ; mà là chi phí thật của máy bay không người lái bị rải ra bên ngoài thân máy bay. Việc huấn luyện con người, nhân viên bảo

trì, mạng liên lạc, pin, thiết bị truyền và nhận video, cùng tỷ lệ tiêu hao cũng như vậy.

Tỷ lệ hao hụt là trục của phép tính này. Khi đã xác định mỗi tháng mất bao nhiêu chiếc, khung máy bay giá rẻ không còn là vật tiêu hao dùng một lần nữa, mà trở thành khoản chi lặp lại hằng tháng. Nếu một đơn vị mất 100 drone trong một tháng, mỗi chiếc 500 đô la, chi phí drone của đơn vị đó là 50.000 đô la mỗi tháng. Chỉ xem đoạn video về một chiếc drone phá hủy một xe tăng thì câu hỏi về chi phí vẫn chưa có lời đáp. Giá của hàng chục chiếc không tới được mục tiêu cũng phải được tính vào. Toàn bộ khoản đó mới là cái giá thật đã đổ vào một lần thành công. Việc nguồn cung đầu đạn và chất nổ do drone cảm tử mang theo làm giá ấy tăng thêm bao nhiêu không thể đưa ra con số từ hồ sơ công khai, nên phần đó được để trống.

Ngành công nghiệp kể cùng một câu chuyện bằng một ngôn ngữ khác. Kyiv School of Economics Institute và Brave1 công bố "Ukraine's Drone Industry: Investment and Product Innovation" vào ngày 4 October 2024. Báo cáo phân tích ngành drone với trọng tâm là đầu tư và doanh thu. Báo cáo nêu khoản đầu tư 15 triệu đô la mà startup Ukraina Swarmer huy động được, cùng các chỉ số doanh thu của công ty này. Swarmer là công ty xây dựng công nghệ bay tự hành theo đàn. Nguồn của biểu đồ đó được ghi là UNITED24.

Nguồn của các thống kê về ngành drone phần lớn là một nền tảng của chính phủ. Dòng tiền của ngành drone đi qua một nền tảng chính phủ, và ngay cả dữ liệu dùng để phân tích ngành này cũng dựa vào các con số tổng hợp của chính nền tảng đó. Khi vòng vận hành chạy tốt, đó là hiệu quả. Tiền và thông tin nằm ở một nơi, nên quyết định được đưa ra nhanh. Nhưng khi tài liệu kiểm chứng từ bên ngoài còn ít, một khi có chuyện trục trặc thì rất khó tìm nguyên nhân, vì cơ quan xây dựng hệ thống cũng tự đánh giá kết quả của chính mình.

Thực tế sản xuất cũng không trơn tru như các thông báo. Các công ty mới chỉ tham gia thị trường sau khi chính phủ nới trần biên lợi nhuận. Sau đó, nhà nước còn cắt bớt giấy tờ thử nghiệm và chứng nhận. Nhà nước bố trí nhân sự chuyên trách để giúp doanh nghiệp đăng ký mã với Ministry of Defense. Ghi nhận rằng dịch vụ hậu mãi của các nhà sản xuất không theo kịp, buộc các đơn vị phải tự lập đội sửa chữa, cũng thuộc cùng bức tranh ấy. Xây nhà máy là chưa đủ. Để những drone đã sản xuất tiếp tục hoạt động ở tiền tuyến, phải có đào tạo, sửa chữa và nguồn cung linh kiện đi theo. Ukraina đã gặp khó khăn nghiêm trọng ở đoạn vận hành này.

Trước chiến tranh điện tử, điều chúng ta biết và điều chúng ta chưa biết phải được tách riêng. Thứ thật sự quyết định tuổi thọ của một chiếc drone giá rẻ không phải là xe tăng của đối phương, mà là hoạt động gây nhiễu của đối phương. Công nghệ này, gọi là jamming, hoạt động bằng cách phủ tiếng ồn nặng lên sóng vô tuyến đi qua lại giữa drone và phi công cho đến khi tín hiệu bị đứt. Khi tín hiệu định vị vệ tinh cũng bị cắt theo, thân máy bay không còn biết mình đang ở đâu, và ngay cả một chiếc drone được chế tạo tốt cũng rơi khỏi vị trí đó. Những drone gửi tín hiệu điều khiển qua cáp quang xuất hiện để tránh jamming. Công nghệ dẫn

đường cho phép drone tự bay đoạn cuối tới mục tiêu mà không cần con người điều khiển cũng đã xuất hiện.

Nhưng trong các tài liệu được dùng làm nền tảng ở đây, những con số chứng minh tỷ lệ thành công của jamming, tỷ trọng drone cáp quang, và quy mô áp dụng dẫn đường tự động, hồ sơ công khai dừng lại tại đây. Điều nằm ngoài hồ sơ công khai không thể được viết như thể đã được xác nhận, nên khoảng trống này được giữ nguyên. Việc jamming là một biến số trung tâm của cuộc chiến drone, và việc chúng ta chưa thể nói về độ lớn của biến số đó bằng con số, cả hai đều phải được ghi lại cùng nhau.

Điều có thể ghi lại thay vào đó là cuộc tranh luận này đang diễn ra ở đâu. Australian Army Research Centre công bố "Drones in Modern Warfare: Lessons Learned from the War in Ukraine" vào ngày 22 October 2024. American Irregular Warfare Center phát hành "Six Lessons from Ukraine's Drone War" vào ngày 20 May 2026. Chính việc quân đội nhiều nước đang sắp xếp drone trong cuộc chiến này dưới tiêu đề "lessons" đã là một sự kiện. Trong những thứ Ukraine tạo ra, bên cạnh vũ khí, còn có một cuốn giáo trình mà các nước khác mở ra khi thiết kế lại quân đội của mình. Hai báo cáo đó có đi đến cùng kết luận với các thông báo của chính phủ Ukraine hay không là câu hỏi chỉ có thể trả lời sau khi so sánh từng tài liệu một.

Cần vạch rõ một ranh giới. Army of Drones không phải là một đội hình quân sự. Đó là một chương trình mua sắm và huy động, dùng tiền quyên góp và ngân sách nhà nước để mua drone rồi gửi tới các đơn vị, đào tạo phi công, và chuyển kết quả thành điểm để hỗ trợ thay thế. Brave1 là một tổ chức hỗ trợ các startup công nghệ quốc phòng. Unmanned Systems Forces là một binh chủng chính thức, tập hợp những binh sĩ vận hành drone, và được thành lập sau Brave1. Ba thực thể này thường được tin tức giới thiệu gộp lại thành một, nhưng thời điểm ra đời, thẩm quyền, và những người chịu trách nhiệm của chúng đều khác nhau. Bỏ lỡ sự phân biệt này thì thành tích của một người sẽ bị thổi phồng, hoặc trách nhiệm của người khác sẽ bị xóa đi.

Vì vậy, câu chuyện bắt đầu trên sân khấu Cannes vào mùa hè năm 2022 không kết thúc như một câu chuyện thành công, cũng không phải một câu chuyện thất bại. Những khoản quyên góp từ khắp thế giới đã biến thành các đơn đặt hàng trị giá 200 triệu hryvnia chỉ trong ba ngày. Hợp đồng được ký với các nhà sản xuất Ukraina. Sau đó, một mạng lưới đào tạo phi công và một hệ thống thay thế thiết bị dựa trên hiệu suất được xây dựng. Chính vòng vận hành ấy cũng để lại một lỗ hổng hút tiền lương của binh sĩ vào hóa đơn sửa chữa, và để lại một khoảng trống trong khâu kiểm chứng, nơi bên tạo ra kết quả lại tự chấm điểm kết quả của mình.

Fedorov đóng vai trò trung tâm trong việc xây dựng kênh mua sắm này. Nhưng thứ ông xây dựng là một tuyến phụ trợ giúp Bộ Quốc phòng, hay là một tuyến chính đang hướng tới việc thay thế bộ này, vẫn là câu hỏi chưa có lời đáp.

Những chi phí nằm ngoài giá ghi trên khung máy bay còn bao gồm cả mạng thông tin liên lạc. Thứ vận hành Kropyva và Delta, các phần mềm chỉ huy, kiểm soát và nhận thức tình huống của quân đội Ukraina, là internet vệ tinh Starlink; một thiết bị đầu cuối có thể được lắp đặt ở tiền tuyến trong mười lăm phút. Một báo cáo phân tích ghi nhận rằng nhờ kết nối này, thời gian từ lúc drone phát hiện đối phương đến khi pháo binh hoặc drone FPV tấn công đã giảm xuống dưới năm phút. Số thiết bị đầu cuối tăng từ khoảng 42.000 vào đầu năm 2023 lên khoảng 200.000 vào khoảng tháng 10 năm 2025. Để một khung máy bay 500 đô la đánh trúng mục tiêu, phía sau nó phải có một mạng thông tin vệ tinh ở quy mô như vậy.

Tổ hợp giá rẻ ấy không chỉ được một bên sử dụng. Quân đội Nga đã gắn các thiết bị đầu cuối Starlink, được tuồn qua các nước thứ ba, lên drone cảm tử Shahed do Iran sản xuất. Những khung máy bay được cải biến theo cách này có thể trao đổi tài liệu theo thời gian thực từ khoảng cách xa tới 2.000 kilometer. Điều đó có nghĩa là chúng có thể tấn công sâu vào hậu phương Ukraina. Tổ hợp mà Ukraina tìm ra trước cũng đã được dùng theo chiều ngược lại.

Vì vậy, điều làm cho cụm từ "drone giá rẻ" trở nên chông chênh không phải là giá của khung máy bay. Chi phí thật sự của một chiếc drone bao gồm cả việc đào tạo phi công và các hóa đơn sửa chữa mà đơn vị phải trả. Chi phí của các thiết bị đầu cuối vệ tinh ở tiền tuyến cũng khó có thể tách ra. Không có tài liệu nào được thu thập mà đồng thời tính cả rủi ro rằng đối phương có thể dùng chính những thiết bị đầu cuối ấy. Điều chúng ta biết là tên của từng khoản mục, chứ không phải tổng số của chúng.

Chương 7. Brave1, một Thung lũng Silicon quốc phòng giữa chiến tranh

Brave1 là một tổ chức hỗ trợ công nghệ quốc phòng do chính phủ Ukraine thành lập. Theo trang web chính thức của tổ chức này, tính đến ngày 13 July 2026, Brave1 có 2,500 công ty thành viên và hơn 5,000 sản phẩm đã đăng ký. Số nhà sản xuất thiết bị bay không người lái vượt quá 500, còn các nhà sản xuất trí tuệ nhân tạo và phương tiện mặt đất không người lái đều vượt quá 200 trong từng nhóm. Brave1 đóng vai trò là cổng kết nối các công ty với quân đội, chính phủ và nhà đầu tư.

Những con số này là thống kê riêng của Brave1, do chính Brave1 công bố. Trên trang web không có dấu hiệu nào cho thấy một công ty kế toán bên ngoài hoặc một cơ quan kiểm toán đã xác minh chúng. Hồ sơ công khai dừng lại ở đây.

1. Quy tụ các startup, quân đội, chính phủ và nhà đầu tư vào một nơi

Thị trường công nghệ quốc phòng của Ukraine vào năm 2022 rất sôi động, nhưng phân tán. Ngày càng nhiều người lắp ráp drone trong gara và căn hộ, còn các công ty phần mềm từng làm ứng dụng và trò chơi trong thời bình bắt đầu viết chương trình cho chiến trường. Rắc rối xuất hiện ở bước tiếp theo. Không có một cổng chính thức để giới thiệu thứ mình đã chế tạo cho quân đội, và thứ nối các đơn vị tiền tuyến với nhà phát triển phần lớn là lời giới thiệu cá nhân hoặc một bài đăng trên mạng xã hội.

Khi không có một kênh chính thức giữa các nhà phát triển và quân đội, ngay cả việc thử nghiệm một sản phẩm cũng khó. Giả sử một nhà phát triển chế tạo được một mô-đun liên lạc có thể chịu được tác chiến gây nhiễu của đối phương. Anh ta không có cách nào biết thiết bị của mình có thật sự tốt hay không. Chỉ một đơn vị ở tiền tuyến mới có thể đánh giá điều đó, nhưng anh ta lại không có cách nào biết đơn vị ấy ở đâu hoặc phải liên hệ với ai. Phía bên kia cũng gặp đúng bức tường ấy. Một đại đội trưởng ở tiền tuyến chiến đấu mà không biết rằng chính thiết bị ông cần hôm nay đã tồn tại dưới dạng nguyên mẫu hoàn chỉnh ở một góc xưởng nào đó. Công nghệ và nhu cầu cùng nằm trong một quốc gia, vậy mà chúng không tìm được nhau, và cái giá của sự lệch pha ấy được trả ở tiền tuyến.

Brave1 là cơ chế được dựng lên để các nhà phát triển và quân đội gặp nhau tại một cửa duy nhất. Tháng 4 năm 2023, chính phủ Ukraine ra mắt cụm công nghệ quốc phòng này. Các tài liệu giới thiệu của chính phủ nói rằng sáu bộ đã tham gia. Tuy nhiên, chỉ có năm cơ quan tham gia có thể được xác định bằng tên: Ministry of Digital Transformation, Ministry of Defense, General Staff, National Security and Defense Council, và Ministry of Economy. Trong số này, General Staff và National Security and Defense Council là các cơ quan quân sự và an ninh, không có địa vị là bộ trong chính phủ. Cơ quan thứ sáu là cơ quan nào, và liệu con số "sáu" của chính phủ có

tính gộp cả các bộ và các cơ quan khác hay không, không thể được xác nhận trong các tài liệu công khai mà phần trình bày này dựa vào. Thay vì chép nguyên một con số như thể nó đã rõ ràng, chúng ta đánh dấu phần nằm ngoài hồ sơ công khai đúng là nằm ngoài hồ sơ công khai.

Điều có thể xác nhận nằm ở tầng bên dưới. Brave1 là một chương trình quốc gia do nhiều cơ quan chính phủ cùng tạo ra, và phạm vi tham gia rộng như vậy khiến việc gọi nó là sản phẩm của riêng Mykhailo Fedorov trở nên gượng ép. Ministry of Digital Transformation đứng ở trung tâm vận hành, nhưng Ministry of Defense, General Staff, National Security and Defense Council, và Ministry of Economy gắn chặt với nó trong các vấn đề mua sắm và quy định. Ngay khi tổ chức này được gọi bằng tên của một cá nhân, trách nhiệm mà nhiều cơ quan đã chia nhau cũng bị dồn lên một người ấy. Công lao được chia sẻ thì trách nhiệm khi có sai sót cũng có thể được chia sẻ, và trong bộ máy hành chính thời chiến, chính sự phân biệt này là nơi mọi cuộc kiểm toán về sau bắt đầu.

Hãy nhìn vào hình thức pháp lý của nó. Brave1 không có địa vị của một pháp nhân riêng biệt, độc lập. Nó là một chương trình quốc gia và một thị trường vận hành bên trong Innovation Development Fund thuộc Ministry of Digital Transformation. Nó giữ vai trò lửng lơ của một nền tảng nằm trong một cơ quan chính phủ, và chính trạng thái lửng lơ ấy về sau lại trở thành vấn đề. Một công ty có cổ đông và kiểm toán viên kiểm tra sổ sách. Một đơn vị quân đội có chuỗi chỉ huy và các thanh tra quân sự bám sát. Một nền tảng bên trong chính phủ lại không rơi gọn vào mạng lưới nào trong hai mạng lưới ấy, và vì thế càng khó xác định nghĩa vụ kiểm toán nằm ở đâu.

Nền tảng này đảm nhận việc tiếp nhận và thử nghiệm sản phẩm, cũng như cung cấp tài chính. Công việc của nó là dựng một cửa vào, cấp khoản tiền ban đầu, và kéo vốn tư nhân tham gia.

Hãy bắt đầu từ cửa vào. Một phân tích của Viện Quan hệ Quốc tế Pháp (IFRI) mô tả Brave1 là cửa vào chính, nơi hơn 2.000 startup tư nhân cùng các doanh nghiệp nhỏ và vừa đi qua để tìm hỗ trợ của chính phủ và nhà đầu tư. Trước đây, một nhà phát triển không biết phải gõ cửa phòng nào của Bộ Quốc phòng; giờ đây chỉ còn một cánh cửa để gõ. Việc chỉ có một cánh cửa đem lại tiện lợi, nhưng đồng thời cũng là một mối nguy, vì phán đoán của những người canh cánh cửa đó sẽ quyết định số phận của cả thị trường. Không có phương pháp nào được đặt ra để sau này xác định liệu một công nghệ bị loại trong quá trình xét duyệt thật sự kém, hay con mắt của người xét duyệt quá hẹp.

Việc nhà nước cấp khoản tiền ban đầu là một vấn đề khác về bản chất. Các startup phần cứng gặp khó khi vay ngân hàng. Ở giai đoạn chưa ai biết nguyên mẫu sẽ bay lên hay phát nổ, tức là một công ty ở mức độ sẵn sàng công nghệ từ 1 đến 5, rất hiếm ngân hàng sẵn sàng cho vay, dù trong thời chiến hay thời bình. Mức độ sẵn sàng công nghệ là thang đo chia quãng đường từ một ý tưởng đến triển khai trên chiến trường thành chín bậc. Bậc một là nguyên lý trên giấy;

bậc chín là sản phẩm hoàn chỉnh đã được chứng minh trong chiến đấu thực tế. Các bậc 1 đến 5 có nghĩa là chưa có gì được chứng minh. Đó là đoạn mà vốn sợ nhất, và cũng là đoạn bị bỏ trống ở khắp nơi trên thế giới. Vì vậy các nhà sáng lập gọi nó là thung lũng chết. Ý tưởng còn sống nhưng không có tiền, nên nó chết ngay trước nguyên mẫu, và công nghệ chết theo cách đó thậm chí không bao giờ xuất hiện trong thống kê.

Brave1 lấp vào vai trò đó bằng hỗ trợ không hoàn trả, tức là bằng các khoản tài trợ. Tài trợ là tiền được cấp mà không có nghĩa vụ trả lại. Nếu công ty thất bại, khoản tiền không được thu hồi; nếu công ty thành công, nhà nước không lấy cổ phần. Đổi lại có một điều kiện: trong một thời hạn xác định, công ty phải bàn giao nguyên mẫu đạt mức hiệu năng đã nêu. Tính đến tháng 9 năm 2024, 329 khoản tài trợ đã được chi trả, với tổng giá trị năm triệu đô la. Sang năm 2025, quy mô thay đổi. Tài chính tài trợ vượt sáu mươi triệu đô la và mở rộng tới hơn 600 công ty, còn ngân sách quốc gia năm 2025 dành riêng khoảng 71,6 triệu đô la cho các khoản tài trợ của Brave1. Các nhà phát triển có thể nộp đơn xin từ khoảng 12.000 đô la đến tối đa 192.000 đô la, tùy theo tầm quan trọng của dự án. Từ năm triệu đô la lên sáu mươi triệu: tăng hơn mười lần chỉ trong một năm.

Tháng 9 năm 2025, trong một cuộc phỏng vấn với một kênh quân sự Ukraine, Mykhailo Fedorov gọi Brave1 là "nhà đầu tư thiên thần lớn nhất của Ukraine". Nhà đầu tư thiên thần là một cá nhân bỏ tiền riêng vào một công ty ở giai đoạn sớm nhất, khi công ty chưa có doanh thu, cũng chưa có sản phẩm. Ở Silicon Valley, những nhà sáng lập đã thành công và các giám đốc điều hành đã nghỉ hưu thường nhận vai trò đó. Họ tính theo phép toán này: nếu rót vốn cho mười công ty, chín công ty có thể thất bại, miễn là một công ty thành công thật lớn. Tuyên bố của Fedorov có nghĩa là nhà nước đã nhận lấy vai trò đó. Nghe như một lời khoe, nhưng nó cũng có nghĩa là phần rủi ro mà vốn tư nhân không muốn gánh đang được chuyển sang tiền thuế. Một nhà đầu tư thiên thần trả tiền cho chín thất bại bằng túi tiền của chính mình. Khi nhà nước tự gọi mình là nhà đầu tư thiên thần, công dân trả tiền cho chín thất bại ấy, và hóa đơn được hòa vào ngân sách mà không bao giờ đặt lên bàn của bất kỳ ai.

Nhiệm vụ cuối cùng là kéo vốn tư nhân vào. Brave1 duy trì một cơ sở dữ liệu gồm hơn 150 quỹ đầu tư mạo hiểm và thường xuyên tổ chức các ngày trình diễn, nơi các công ty có thể trình bày trực tiếp với nhà đầu tư. Oleksandr Bornyakov, thứ trưởng Bộ Chuyển đổi số, đã kể lại giai đoạn đầu ảm đạm đến mức nào. Đầu năm 2023, ông nói, không ai muốn đầu tư vào công nghệ quốc phòng, nên họ phải đi khắp châu Âu và Hoa Kỳ để trực tiếp giải thích. Theo lời ông, chính phủ Ukraine đã ra nước ngoài để bảo chứng cho mức độ đáng tin cậy của chính các nhà sáng lập trong nước. Cụm này tự đặt mình vào vai trò người dẫn đường qua hệ thống hành chính phức tạp của Ukraine, đồng thời thẩm tra lai lịch của các nhà sáng lập để những đội ngũ đáng tin cậy có thể được nối với các nhà đầu tư nước ngoài.

Thời gian trôi qua, danh sách tham gia dần đầy lên. Các quỹ như D3 Venture Capital, nơi cựu giám đốc điều hành Google Eric Schmidt tham gia với tư cách đối tác, cùng với MITS Capital, Green Flag Ventures, và Nezlamni, quỹ do công ty gọi xe Uklon lập ra, đã bước vào hệ sinh thái này. Ukraine, ở năm thứ ba của cuộc chiến, đã được đánh dấu như một tọa độ trên bản đồ vốn đầu tư mạo hiểm quốc tế.

Các bảng điểm dành cho từng công ty cũng bắt đầu xuất hiện. Swarmer, công ty xây dựng trí tuệ nhân tạo cho các đàn drone, nhận các khoản tài trợ 50.000 dollars rồi 200.000 dollars từ Brave1, chứng minh được công nghệ của mình, sau đó gọi được 2,7 triệu dollars vốn đầu tư seed, và đến năm 2025 gọi được vòng Series A trị giá 15 triệu dollars. Đầu tư seed là khoản tiền đầu tiên ở giai đoạn gieo hạt; Series A là khoản tiền để mở rộng cánh đồng khi hạt giống ấy đã nảy mầm. Con đường Swarmer đã đi, xây dựng nguyên mẫu bằng tài trợ của nhà nước, rồi đứng trước vốn tư nhân với kết quả trong tay, là mẫu hình tiêu biểu của mạch mà Brave1 thiết kế. Osavul, một công ty trí tuệ nhân tạo chống thông tin sai lệch, gọi được ba triệu dollars, còn Farsight Vision, một nền tảng tình báo chiến trường, gọi được 600.000 euros. Bornyakov nói một hệ sinh thái gồm vài trăm nhà đầu tư thiên thần đã hình thành, và nhìn xa hơn mốc chín mươi triệu dollars tới mức đầu tư mạo hiểm khoảng 150 đến 200 triệu. Con số cuối cùng đó là dự báo của ông, không phải kết quả đã có.

Những con số được đưa ra đến đây đều là các con số hướng vào bên trong, nói về "tiền đã rót vào" và "các công ty đã quy tụ": số tiền tài trợ, số lượng công ty, số lượng sản phẩm, vốn đầu tư huy động được. Chúng không nói gì về những gì đã bị phá hủy ngoài mặt trận, hay mức độ phá hủy là bao nhiêu. Vốn đầu tư huy động được là chỉ dấu cho thấy thị trường định giá công nghệ của quốc gia này ra sao, còn bằng chứng rằng công nghệ ấy thật sự hoạt động phải đến từ nơi khác. Những công ty được các tài liệu về Brave1 nêu như câu chuyện thành công, phần lớn, được mô tả là thành công dựa trên các vòng gọi vốn của họ. Việc một nhà đầu tư đặt cược và việc mạng sống của một người lính được cứu là hai câu khác nhau, và không thể xóa nhòa sự khác biệt ấy khi đi qua.

Tên của các công ty nhận tài trợ vẫn còn trong các tài liệu công khai. DeepState, Swarmer, Skylab, Mantis Analytics, và Frontline đã dùng khoản tiền này cho phát triển sản phẩm giai đoạn đầu và kiểm tra hiệu năng. Phía còn để lại tên là phía đã sống sót. Tên của một công ty nhận tài trợ rồi dừng lại trước nguyên mẫu của mình không xuất hiện trong danh sách nào, và liệu một danh sách như vậy từng được lập hay chưa, hồ sơ công khai dừng lại ở đây.

So sánh các khoản tài trợ với đầu tư tư nhân cho thấy quy mô của khoản tiền ban đầu mà nhà nước đã gánh lấy. D3 Venture Capital, với quỹ từ 19 đến 30 triệu đô la, rót từ 125.000 đến 750.000 đô la vào một công ty. MITS Capital, ở quy mô 50 triệu đô la, rót từ 100.000 đến 500.000 đô la. Mức trần tài trợ 192.000 đô la của Brave1 có quy mô tương đương một khoản đầu tư tư nhân giai đoạn đầu như vậy. Nhà nước ngồi vào bàn với khoản tiền xấp xỉ quy mô của một nhà

đầu tư tư nhân, và khác biệt duy nhất là nhà nước không lấy cổ phần.

Vòng hạt giống của Swarmer đã thu hút công ty quốc phòng Mỹ R-G.AI, cùng với Radius Capital, Green Flag Ventures, và D3, và vào tháng 2 năm 2026 công ty đã nộp hồ sơ niêm yết trên Nasdaq, trở thành công ty công nghệ quốc phòng Ukraine đầu tiên làm việc này. Một công ty được nhà nước chuẩn bị bằng 50.000 và 200.000 đô la đang gõ cửa thị trường chứng khoán Mỹ. Nếu việc niêm yết diễn ra, lợi ích sẽ thuộc về các cổ đông. Ngân khố Ukraine, bên đã gánh rủi ro ban đầu, lấy lại phần của mình trong khoản lợi ấy bằng cách nào, hay có nhận lại được gì hay không, điều đó không xuất hiện trong các tài liệu công khai.

Việc thẩm định mà Bornyakov mô tả cũng đáng được nhìn lại kỹ hơn. Cụm này kiểm tra lý lịch của các nhà sáng lập và chỉ kết nối những đội đáng tin cậy với nhà đầu tư nước ngoài. Với nhà đầu tư, điều đó gần như có nghĩa là rủi ro của một quốc gia xa lạ đã được chính chính phủ nước đó lọc trước. Nhìn theo chiều ngược lại, điều đó cũng có nghĩa là vẫn chưa có câu trả lời rõ ràng về việc trách nhiệm sẽ thuộc về ai nếu một đội do chính phủ chọn sau này gây ra rắc rối. Khi nhà nước đứng ra như một bên bảo chứng, uy tín của nhà nước sẽ lên xuống cùng với công ty.

2. Một thử nghiệm thể chế đã thay đổi tốc độ thử nghiệm, chứng nhận và hợp đồng

Cụm này được lập ra để rút ngắn thời gian cần thiết trước khi một sản phẩm đến được một đơn vị. Để một vũ khí đi vào quân đội, thông thường nó phải đi qua một thủ tục dài. Nó phải được thử nghiệm, được kiểm tra theo thông số kỹ thuật, được ghi vào sổ đăng ký, được ký hợp đồng, rồi ngân sách mới được giải ngân. Mỗi bước đều có lý do tồn tại. Nếu thiết bị chưa được kiểm chứng được đặt vào tay một người lính, người lính đó có thể chết. Nếu ngân sách chảy đến một nhà cung cấp chưa được thẩm định, số tiền đó có thể biến mất. Thủ tục chậm là để ngăn tai nạn, và trong thời bình, con đường này kéo dài vài năm cũng không có gì lạ.

Tuổi thọ của công nghệ trên chiến trường drone ngắn hơn thế rất nhiều. Nếu phía bên kia thay đổi tần số của thiết bị tác chiến điện tử, một khung bay hôm qua còn bay hoàn hảo hôm nay có thể rơi xuống. Tác chiến điện tử là cuộc đối đầu trong đó sóng vô tuyến trở thành vũ khí. Nó gây nhiễu tín hiệu vô tuyến nối drone với người điều khiển, hoặc bơm dữ liệu vị trí giả để làm khung bay rơi. Bàn cờ của cuộc chơi này thay đổi theo từng tuần. Khi tốc độ của thủ tục và tốc độ của chiến trường lệch nhau, một vũ khí vượt qua được thủ tục lại mất công dụng ngay trong lúc đang đi qua thủ tục đó. Vào ngày một drone đã được xác minh hoàn hảo trong ba năm theo quy định được triển khai, drone ấy đã là một vật thể lỗi thời.

Chính sự lệch pha này là điểm Brave1 can thiệp, và tổ chức này can thiệp vào hai việc.

Trước hết, Brave1 đưa quân đội ngồi vào bàn thẩm định. Các hồ sơ nộp cho cluster được đại diện của lực lượng quốc phòng cùng xem xét. Sản phẩm được sàng lọc theo nhu cầu của tiền tuyến, rồi những sản phẩm được chọn sẽ được hỗ trợ qua khâu thử nghiệm và mã hóa trang bị

theo chuẩn NATO. Mã hóa là việc gán cho mỗi món trang bị một số định danh riêng phù hợp với chuẩn quốc tế. Hãy nghĩ đến mã vạch trên hàng hóa quanh chúng ta, sẽ dễ hiểu hơn. Không có con số đó, một món hàng không thể đi vào hệ thống tiếp tế của đồng minh, và cũng khó lọt vào danh mục mua sắm chính thức. Nhìn qua thì giống giấy tờ vụn vặt, nhưng chính con số này giúp một vật thể bước lên thành hợp đồng. Sáng chế là việc của kỹ thuật, còn con số là việc của bộ máy hành chính; khi hai thứ không gặp nhau, sáng chế vẫn nằm trong kho.

Sau đó là chợ mua sắm. Ngày 28 April 2025, Brave1 Market mở cửa. Đây là một catalog trực tuyến và kênh mua sắm, nơi các đơn vị quân đội Ukraine có thể trực tiếp tìm kiếm và đặt mua sản phẩm công nghệ quốc phòng. Một cấu trúc cho phép đơn vị đặt hàng thẳng từ nhà sản xuất có nghĩa là bỏ qua vài nấc phê duyệt ở giữa. Thay vì một hồ sơ phải leo từ lữ đoàn lên sư đoàn, từ sư đoàn sang một cục nào đó của Ministry of Defense rồi tiếp tục sang một phòng ban khác, vừa đi vừa gom dấu, một đơn vị có thể chọn thiết bị của mình ngay trên màn hình. Điều đáng ghi nhận là Brave1 đã cố xâu thẩm định, thử nghiệm, mã hóa và đặt hàng vào cùng một tuyến.

Hệ thống được thiết kế như vậy, nhưng kết quả thực tế phải được xác nhận riêng. Điều có thể xác nhận là một thủ tục mới đã được tạo ra; còn thủ tục đó có thật sự biến nhiều tháng thành vài ngày hay không lại là chuyện khác. Trong các tài liệu làm nền cho phần trình bày này, không có phép đo độc lập nào cho thấy trước khi Brave1 can thiệp thì mất bao nhiêu ngày để đi tới hợp đồng, và sau đó mất bao nhiêu ngày. Chỉ có thông báo của chính cluster rằng mọi việc đã nhanh hơn, cùng các báo cáo phân tích trích dẫn thông báo của chính phủ. Muốn xác nhận tốc độ được cải thiện bằng số liệu, cần có thống kê của cơ quan mua sắm về thời gian xử lý hợp đồng, trong khi một phần đáng kể thông tin mua sắm thời chiến bị giữ lại vì lý do an ninh.

Cũng không có cơ sở nào để gọi câu “nó đã nhanh hơn” là sai. Câu đó có nghĩa là tuyên bố ấy chưa được kiểm chứng; câu thứ nhất là một lời phản bác, còn câu thứ hai là một sự dè dặt. Khi một chính phủ đang trong chiến tranh báo cáo về kết quả chính sách của chính mình, bản báo cáo thường chỉ về hướng của sự thật nhưng không chỉ chính xác quy mô của sự thật ấy. Người đọc có quyền đọc hướng đi và quy mô như hai vấn đề riêng.

Những con mắt bên ngoài không hoàn toàn vắng mặt. Tháng 10 năm 2023, Center for Security and Emerging Technology (CSET) tại Georgetown University công bố một báo cáo về một hội nghị drone do U.S. Defense Innovation Unit (DIU) và Brave1 cùng tổ chức tại Warsaw. Điều đó có nghĩa là sáu tháng sau khi cụm này ra đời, một tổ chức nghiên cứu chính sách phương Tây đã bắt đầu xem hệ sinh thái drone của Ukraine là đối tượng quan sát trực tiếp. Thí nghiệm thể chế của Ukraine ngay từ đầu đã diễn ra trước sự theo dõi quốc tế. Quan sát không phải là kiểm toán, nhưng vẫn tốt hơn là không có ai nhìn vào.

Còn một sự thật nữa phải được đặt bên cạnh mọi đánh giá về giá trị của thí nghiệm này. Brave1 không thay thế hệ thống mua sắm công. Đây là một kênh tồn tại tách biệt với quy trình

mua sắm chính thức của Ministry of Defense, gần giống một khoảng sân dẫn vào mua sắm chính thức. Vì vậy, dù cụm này chạy nhanh đến đâu, nếu cánh cửa ngân sách và hợp đồng bị chặn ở chặng cuối, hàng hóa vẫn không đến được tiền tuyến. Các phân tích về năng lực sản xuất drone đã chỉ ra rằng nút thắt của Ukraine đã chuyển từ việc có thể chế tạo hay không sang việc có tiền để mua hay không. Nút thắt đó nằm ngoài thiết kế của Brave1. Ngay cả sau khi chính phủ tăng tốc độ chế tạo, tốc độ mua vẫn là vấn đề ngân sách, và riêng cụm này không thể gỡ được tình trạng các nhà máy vẫn chạy nhưng đơn đặt hàng không đến.

Brave1 đã biến con đường để một nhà phát triển gặp quân đội thành một thiết chế, còn việc con đường ấy đã rút ngắn tổng thời gian mua sắm đến mức nào thì với các tài liệu hiện được công khai, hồ sơ công cộng dừng lại ở đây.

Khối lượng tài liệu được đưa lên bàn thẩm định không hề nhỏ. Các tài liệu về cụm này ghi rằng hơn 900 hồ sơ đã được xử lý chỉ trong một năm. Những người thẩm định là đại diện của lực lượng quốc phòng. Nguyên tắc người sẽ sử dụng vũ khí là người chọn vũ khí gần với lẽ thường, và đối với nhà phát triển, yêu cầu từ tiền tuyến trở thành chính bản đặc tả kỹ thuật. Đổi lại, tiêu chuẩn này chỉ nhìn trong một khoảng thời gian hẹp. Khi thứ tiền tuyến muốn hôm nay khác với thứ sẽ cần sau hai năm nữa, không có phương pháp nào được đặt ra để từ hồ sơ xác nhận xem bên nào trong hai nhu cầu ấy bị đẩy xuống sau.

Mở cụm từ "các đơn vị đặt hàng trực tiếp" ra, bên trong là một hệ thống điểm. Các đơn vị tiền tuyến tích lũy điểm nhờ kết quả tấn công đã được xác nhận, và bằng số điểm ấy họ đặt mua drone và thiết bị trực tiếp từ các nhà sản xuất trên Brave1 Market. Điều đó có nghĩa là một đơn vị chọn thiết bị của mình trên màn hình mà không phải đi qua chuỗi phê duyệt của Bộ Quốc phòng. Một phần quyền quyết định mua sắm đã đi từ đỉnh chuỗi chỉ huy xuống tận cấp dưới.

Một phương pháp tăng nguồn cung theo kết quả chiến trường cũng có tác dụng phụ. Điểm được tích lũy thông qua các cuộc tấn công. Một đơn vị được giao nhiệm vụ trinh sát, chuyển tiếp thông tin liên lạc, sơ tán thương binh, hoặc phòng thủ vị trí, tức những nhiệm vụ không chuyển thành số lần tấn công, sẽ đứng trước cùng một màn hình với ít điểm hơn. Còn về các tài liệu cho thấy cấu trúc này đã thực sự thay đổi việc phân phối thiết bị giữa các đơn vị ra sao, hồ sơ công khai dừng lại tại đây. Bản thiết kế được công khai, nhưng việc phân phối do bản thiết kế ấy tạo ra vẫn không thể được đếm từ bên ngoài.

Chính phủ Ukraine tuyên bố rằng hơn 80 phần trăm mục tiêu của đối phương bị drone phá hủy, và các báo cáo phân tích dẫn tin Reuters đã truyền lại nguyên vẹn tuyên bố đó. Ở đây cũng vậy, bên đưa ra tuyên bố và bên mà tuyên bố hướng tới không tách rời nhau. Khoảng cách giữa câu nói rằng hệ thống đã nhanh hơn và bằng chứng rằng hệ thống đã hoạt động, từ đầu đến cuối phần này, vẫn chưa được vượt qua.

3. Các chỉ số hiệu quả và khoảng trống nơi lẽ ra phải có kiểm toán bên ngoài

Để đánh giá Brave1, cần tách riêng hai câu hỏi. Cụm này đã công bố điều gì? Và ai đã kiểm chứng công bố đó?

Hãy đặt lại một lần nữa các chỉ số mà Brave1 đã đưa ra. 2.500 công ty, hơn 5.000 sản phẩm, hơn 500 nhà sản xuất máy bay không người lái. Những con số này đều đến từ các bài đăng của chính Brave1. Các khoản tài trợ tăng từ 329 khoản với tổng giá trị năm triệu dollar lên hơn sáu mươi triệu dollar. Một khoản phân bổ ngân sách 71,6 triệu dollar. 150 quỹ đầu tư mạo hiểm. Đây là một danh sách gây chú ý, và từng con số trong đó đều đếm xem đã tập hợp được bao nhiêu và đã chi ra bao nhiêu.

Đây là các chỉ số đầu vào. Trong một trường học, chúng tương ứng với việc đã tuyển bao nhiêu giáo viên và mua bao nhiêu sách. Điểm số của học sinh có tăng hay không là chuyện phải được trả lời bằng những con số khác, và các con số có thể trả lời những câu hỏi sau lại không xuất hiện trong tài liệu công khai. Trong khoảng 600 công ty đã nhận tài trợ, bao nhiêu công ty thực sự giao được sản phẩm cho một đơn vị? Tỷ lệ nào nhận tài trợ nhưng không tạo ra sản phẩm? Trong 5.000 sản phẩm đã đăng ký, bao nhiêu sản phẩm vượt qua thử nghiệm, bao nhiêu sản phẩm đi tới codification, và bao nhiêu sản phẩm dẫn tới hợp đồng? Có khác biệt nào về hiệu quả trên chiến trường giữa các công nghệ được cụm hỗ trợ và các công nghệ không được hỗ trợ hay không?

Những nhà đầu tư mạo hiểm không công bố tỷ lệ thất bại của mình là chuyện thường thấy. Đó là tiền tư nhân, và phán đoán tư nhân có thể giữ nó trong bóng tối. Nhưng số tiền Brave1 chi ra là ngân sách quốc gia. Nếu nhà nước tự gọi mình là nhà đầu tư thiên thần, thì cùng với sự tự do của một nhà đầu tư thiên thần, nhà nước cũng phải gánh các nghĩa vụ của một định chế công. Trong các tài liệu công khai không có báo cáo kế toán hay báo cáo của cơ quan kiểm toán nào kiểm toán độc lập việc Brave1 giải ngân các khoản tài trợ. Khoảng trống này có thể là giới hạn của bộ tài liệu được thu thập, hoặc cũng có thể là chưa hề tồn tại một tài liệu như vậy. Giữa hai khả năng ấy, chúng tôi không vội khép lại kết luận; chúng tôi chỉ giữ lại sự thật rằng khoảng trống đó đang tồn tại.

Để đo kích thước của khoảng trống ấy, cần có một điểm so sánh. Ngay trong Ukraine, trong cùng thời chiến, có một lĩnh vực được trang bị bộ máy kiểm toán dày đặc hơn nhiều: lĩnh vực tái thiết, nơi dòng tiền quốc tế đổ vào.

Quỹ Ủy thác Cứu trợ, Phục hồi, Tái thiết và Cải cách Ukraine (Ukraine Relief, Recovery, Reconstruction and Reform Trust Fund, URTF), do World Bank dẫn dắt, công bố khung kết quả của mình dưới dạng tài liệu. Tính đến năm 2025, quỹ này đã huy động lũy kế 2.52 tỷ dollars và giải ngân 1.5 tỷ, còn các chỉ số tài chính của quỹ được trình bày bằng những cụm từ như mở khóa thêm 4.2 tỷ dollars nhờ sức nâng của khoản hỗ trợ đó. Tất cả các dự án đã được phê

duyệt, tức 100 percent, phải dùng cơ chế giám sát bên thứ ba, và 100 percent phải có sẵn cơ chế khiếu nại của người thụ hưởng.

Hãy bắt đầu bằng cách mở ra cụm từ giám sát bên thứ ba. Đó là một thủ tục trong đó một tổ chức thứ ba, đứng ngoài cả bên đưa tiền lẫn bên nhận tiền, đi đến hiện trường, tự mình xác nhận công việc có thật sự diễn ra hay không, rồi ghi lại trong tài liệu. Nếu giấy tờ nói ba mươi bệnh viện đã được sửa chữa nhưng thực tế chỉ có hai mươi, việc phát hiện khoảng cách ấy là nhiệm vụ của bên thứ ba. Cơ chế khiếu nại là một thiết bị hướng theo chiều ngược lại. Khi những cư dân đáng lẽ được hưởng lợi từ một dự án cảm thấy tiền đã rò rỉ sang nơi khác, một cửa sổ để nộp khiếu nại đã được lập sẵn từ trước. Trong URTF, UDA Consulting phụ trách giám sát bên thứ ba trên toàn danh mục, đến thăm các địa điểm và ghi nhận tiến độ, trong khi các dự án phục hồi logistics và năng lượng tại những khu vực khó tiếp cận hoặc nguy hiểm được United Nations Office for Project Services (UNOPS) giám sát với tư cách trustee agent.

Cũng có những cơ chế trong nước. Việc kiểm toán độc lập đối với chi tiêu công thuộc về Accounting Chamber và State Audit Service, còn các vụ tham nhũng cấp cao được xử lý qua một chuỗi gồm National Anti-Corruption Bureau (NABU), Specialized Anti-Corruption Prosecutor's Office (SAPO) và High Anti-Corruption Court. Nền tảng DREAM, nơi công bố dữ liệu dự án tái thiết từ phân bổ ngân sách đến mua sắm công và tỷ lệ tiến độ, cho phép các nhà tài trợ và xã hội dân sự nhìn thấy cùng những tài liệu mà chính phủ đang nhìn thấy. Giám sát không thể đứng vững nếu thông tin chỉ nằm ở một phía, và trách nhiệm giải trình bắt đầu khi các bên cùng nhìn vào một màn hình.

Xã hội dân sự cũng không ngồi yên. Chỉ riêng trong năm 2025, Anti-Corruption Action Center (ANTAC) đã phân tích 1.526 vụ mua sắm công và nộp đơn khiếu kiện pháp lý đối với mười thủ tục mua sắm có rủi ro tham nhũng đã được xác nhận. Mạng lưới giám sát này trên thực tế đã làm thay đổi diễn biến sự việc. Sau khi bê bối nổ ra về giá bị thổi phồng đối với các mặt hàng như trứng và áo khoác trong mua sắm của Ministry of Defense, luật đã được sửa đổi để đưa mua sắm quốc phòng trở lại nền tảng mua sắm điện tử công khai ProZorro. ProZorro là một hệ thống đưa thẳng lên internet thông tin ai đang mua gì với giá bao nhiêu. Đó là một biện pháp trong đó chính phủ tự thừa nhận rằng tham nhũng đã lớn lên khi cánh cửa ấy bị đóng lại vì lý do bí mật thời chiến, và dù lập luận rằng bí mật là cần thiết có thể đúng, bí mật cũng tự gửi hóa đơn của nó cho bạn.

Quanh Brave1, bộ máy ở quy mô này, hồ sơ công khai dừng lại tại đây. Không có tên của một cơ quan giám sát bên thứ ba, không có báo cáo kiểm toán của Accounting Chamber về việc giải ngân tài trợ, không có tài liệu của xã hội dân sự phân tích ngân sách của cụm này; không thứ nào xuất hiện trong các tài liệu công khai.

Phản biện rằng công nghệ quốc phòng nằm trong những điều kiện khác với các dự án tái thiết là có cơ sở. Ngay khoảnh khắc bạn tiết lộ công ty nào đang chế tạo máy bay không người

lái đánh chặn với hiệu năng ra sao, thông tin đó đã được trao cho đối phương. Các báo cáo về lĩnh vực tái thiết cũng chỉ ra cùng một thế khó. Các nhà tài trợ đòi hỏi mức minh bạch tối đa, còn chính phủ phải giữ mức bí mật tối đa mà hoạt động quân sự đòi hỏi. Hai yêu cầu ấy va thẳng vào nhau.

Va chạm không có nghĩa là phải loại bỏ một bên. Con đường DREAM đã đi là bằng chứng. Đó là kiểm soát truy cập theo tầng: hạn chế quyền truy cập vào dữ liệu vị trí nhạy cảm, trong khi công bố các số liệu tổng hợp và thông tin tiến độ. Công trình nào đang được xây dựng, ở đâu thì được che đi; đã chi bao nhiêu tiền và tiến triển đến đâu thì được hiển thị. Chuyển cùng logic ấy sang công nghệ quốc phòng, kết quả sẽ như sau. Ngay cả khi che giấu công ty nào đang làm sản phẩm nào, vẫn có thể công bố số liệu tổng hợp về bao nhiêu hồ sơ đã vào vòng xét duyệt tài trợ, bao nhiêu hồ sơ được thông qua, và bao nhiêu trong số đó đã đi tới khâu bàn giao. Thông số của một sản phẩm riêng lẻ và tổng khối lượng giải ngân là hai loại thông tin khác nhau, và trong phạm vi có thể kiểm chứng, Brave1 thậm chí đã không mở loại thông tin thứ hai cho việc kiểm tra từ bên ngoài.

Cùng báo cáo về tái thiết ấy chỉ ra một vấn đề đau hơn. Những nơi bộ máy trách nhiệm giải trình yếu nhất lại chính là những nơi rủi ro tham nhũng và phân bổ sai nguồn lực lớn nhất: các khu vực sát tiền tuyến, nơi năng lực giám sát đã cạn kiệt. Nghịch lý này, tức là kiểm soát lỏng ra đúng ở nơi rủi ro cao, cũng lặp lại bên ngoài các công trường tái thiết. Một cấu trúc chi tiền nhanh, ký hợp đồng nhanh, và gửi nhanh ra tiền tuyến, theo định nghĩa, là một cấu trúc cắt bớt các bước kiểm chứng. Khoảnh khắc tốc độ trở thành một đức tính, mọi thủ tục làm chậm lại bắt đầu bị nhìn như vật cản, và một thủ tục đã bị xem là vật cản thì không tồn tại được lâu.

Hồ sơ của Brave1 có thể được chia thành các sự kiện đã được xác nhận và những câu hỏi vẫn nằm ngoài hồ sơ công khai. Những gì đã được xác nhận từ các nguồn là như sau. Một cánh cửa chung đã được mở ra giữa các nhà phát triển và quân đội, những bên trước đó bị phân tán. Tiền nhà nước đi vào giai đoạn đầu nguy hiểm, và vốn đầu tư mạo hiểm nước ngoài đi theo sau. Một kênh chạy từ thử nghiệm và pháp điển hóa cho tới đặt hàng trực tiếp bởi các đơn vị đã được thiết kế thành một định chế. Một quốc gia ở năm thứ ba của cuộc xâm lược đã giành được một tọa độ trên bản đồ đầu tư mạo hiểm quốc tế.

Những gì nằm ngoài hồ sơ công khai là như sau. Hệ thống này thực sự đã rút ngắn thời gian mua sắm đến mức nào. Tỷ lệ thành công và thất bại của các khoản tài trợ mà nhà nước đã rải ra là bao nhiêu. Bao nhiêu trong số 5,000 sản phẩm đăng ký đã tới được tiền tuyến. Và ai, ngoài chính phủ, đã kiểm tra dòng tiền ấy.

Biệt danh "một Thung lũng Silicon quốc phòng bên trong chiến tranh" nắm khá đúng sức nóng của dòng vốn đầu tư và làn sóng lập nghiệp. Chỉ có điều, nhà đầu tư ở Silicon Valley mất tiền của chính họ, còn nhà đầu tư của Brave1 là người dân. Thứ lẽ ra phải lấp đầy khoảng cách ấy là kiểm toán, và kênh đó hiện đang trống. Ghi rõ phần kiểm toán đang thiếu là đang thiếu,

đó là sự lịch sự cao nhất có thể dành cho Brave1 vào lúc này.

Nhìn sâu hơn một chút vào các chỉ số của lĩnh vực tái thiết, hình dạng của cột còn trống trong danh sách của Brave1 hiện ra rõ hơn. Khung kết quả của URTF không chỉ ghi nhận tổng số tiền. Nó ghi rằng đã có lũy kế 40.7 triệu dịch vụ được cung cấp cho người thụ hưởng, 330 cơ sở y tế được sửa chữa thông qua dự án HEAL, 3,130 nhân sự khu vực công được đào tạo cho công tác cứu trợ. Bao nhiêu tiền đã được rót vào, cái gì đã được sửa, và sửa được bao nhiêu, được đếm riêng rẽ. Danh sách Brave1 công bố không có cột nào tương ứng với phần sau.

Các lớp kiểm toán cũng chạy sâu qua nhiều tầng. World Bank không dừng lại ở việc giao xác minh tại hiện trường cho các tổ chức bên ngoài như UDA Consulting và United Nations Office for Project Services; chính họ còn duy trì một ban thanh tra điều tra các vi phạm chính sách và một tổ chức kiểm toán nội bộ bên trong mình. Đó là một cấu trúc trong đó bên đưa tiền nghi ngờ cả chính mình. Anti-Corruption Action Center đã phát hành 339 ấn phẩm trong năm 2025 và nộp ý kiến về mười một dự luật liên quan đến các cơ quan chống tham nhũng, trong đó sáu dự luật được đưa tiếp qua quy trình. Giám sát không vận hành chỉ bằng thiện chí. Nó vận hành khi tài liệu để đọc, một cửa sổ để khiếu nại, và phương tiện pháp lý để tranh chấp cùng tồn tại.

Tiền tái thiết đến từ nước ngoài, nên các nhà tài trợ có thể yêu cầu kiểm toán, và điều kiện gắn giám sát của bên thứ ba vào mọi dự án được phê duyệt đã hình thành theo cách đó. Các khoản tài trợ của Brave1 đến từ ngân sách quốc gia Ukraine. Cách giải thích rằng không có bộ máy kiểm toán đi kèm vì không có nhà tài trợ bên ngoài áp đặt điều kiện nắm khá đúng cấu trúc của sự kiện. Nhưng cách giải thích ấy không làm vấn đề biến mất. Nói rằng không có nhà tài trợ bên ngoài tức là nói chủ sở hữu của số tiền ấy là người dân Ukraine; điều đó không có nghĩa là không có ai đặt điều kiện, mà có nghĩa là những người sẽ đặt điều kiện đang ở bên trong đất nước.

Chương 8. Hệ thống không người lái trở thành một quân chủng, và dòng phát triển DELTA

Ngày 23 tháng 1 năm 2026, một mệnh lệnh xuất hiện trong luồng tin chính thức của Bộ Quốc phòng Ukraine. Văn bản mang chữ ký của bộ trưởng quốc phòng mới, Mykhailo Fedorov, và không liên quan đến việc mua vũ khí hay điều động đơn vị. Mệnh lệnh yêu cầu đưa vào vận hành một hệ thống chỉ huy và kiểm soát drone có tên Mission Control bên trong hệ thống tác chiến mang tên DELTA. Chữ ký ấy được đặt vào ngày thứ chín ông nắm quyền trong tòa nhà bộ.

Một mệnh lệnh lập ra một quân chủng mới, tự nó, chưa làm thay đổi điều gì trên thực địa. Để một câu chữ trên giấy đi tới chiến hào ngoài mặt trận, phải có huấn luyện, thông tin liên lạc và tiếp tế đi theo, và thường phải mất nhiều tháng ở giữa. Nhưng câu chuyện đổi khác khi nhìn vào nền tảng mà văn bản này dựa lên. Mission Control không phải là một hệ thống dựng trên nền đất trống; nó được mô tả như một chức năng đặt lên trên DELTA, hệ thống đã vận hành trong nhiều năm. Việc phát triển và vận hành DELTA do các tổ chức nằm trong quỹ đạo của Bộ Quốc phòng phụ trách, và từ rất lâu trước khi Fedorov tới đó, DELTA đã giữ vai trò bản đồ của quân đội Ukraine.

Trước khi ông trở thành bộ trưởng quốc phòng, hai việc đã cùng lúc tiến lên trong lực lượng vũ trang Ukraine. Một là sự trỗi dậy của drone, từ một thiết bị phụ trợ gắn với các đơn vị khác thành một quân chủng độc lập có tên riêng. Việc còn lại là đặt những gì các drone nhìn thấy lên cùng một lớp với những gì mọi phương tiện giám sát khác nhìn thấy, tất cả trên một màn hình duy nhất. Cũng có thể gọi đó là dựng nên một bàn tay mới và gom các con mắt về làm một. Cả hai dòng chảy ấy đã bén rễ trước khi ông đến, và chính ở đó, phần ông thừa hưởng tách khỏi phần ông tự tay ký.

1. Từ Aerorozvidka đến hệ thống tác chiến DELTA

Trên chiến trường, thông tin không đến từ một nơi duy nhất. Video do drone trinh sát quay, cuộc gọi vô tuyến từ quan sát viên mặt đất, ảnh vệ tinh, dấu vết do radar bắt được, tin báo do cư dân gửi về, tất cả cùng đổ vào một lúc. Vấn đề là những thông tin ấy đi qua các kênh khác nhau, ở các định dạng khác nhau, đến các đơn vị khác nhau. Khi vị trí địch mà một khẩu đội pháo biết không khớp với vị trí mà tiểu đoàn bộ binh bên cạnh biết, cùng một mục tiêu bị đánh hai lần, còn một mục tiêu khác lại bị bỏ sót hoàn toàn. Nếu có nhiều bản đồ, sẽ có nhiều cuộc chiến, và những cuộc chiến ấy cản đường nhau.

DELTA là một hệ thống nhận thức tình huống, thu thập những bản ghi rải rác ấy, xếp chúng lên một bản đồ duy nhất, và cho nhiều đơn vị cùng nhìn vào bản đồ đó cùng lúc. Bộ Quốc phòng Ukraine giới thiệu DELTA như một hệ thống tác chiến được dùng trong toàn lực lượng quốc phòng, và mô tả chức năng của nó là tích hợp nhiều nguồn giám sát cùng báo cáo của các

đơn vị thành một bức tranh chiến trường theo thời gian thực.

Ngay cả thông tin theo thời gian thực cũng không bảo đảm phán đoán chính xác nếu các bản ghi gửi về bị chậm hoặc sai. Điều khiến hệ thống vận hành được là công việc tỉ mỉ: chuẩn hóa các kênh tiếp nhận bản ghi, thống nhất một quy ước ghi tọa độ, và quyết định trước ai có quyền xem nội dung nào. Nếu tọa độ do người điều khiển drone gửi và tọa độ mà kíp pháo đọc không theo cùng một quy tắc, thì màn hình có lộng lẫy đến đâu, bản đồ ấy cũng không thể được tin ngay như nó đang hiện ra. Phần lớn công việc tạo ra một bản đồ chiến trường là công việc hành chính: thỏa thuận quy tắc và khiến mọi người tuân theo.

Khi lần theo nguồn gốc, cái tên thường được nêu làm điểm khởi đầu là Aerorozvidka. Đó là một nhóm kỹ sư dân sự và tình nguyện viên đã tập hợp lại giữa cuộc chiến Donbas năm 2014, tự tay chế tạo drone trinh sát và phần mềm thông tin chiến trường. Cách kể được chấp nhận rộng rãi cho rằng công việc của họ sau đó được đưa vào bộ phận đổi mới của Bộ Quốc phòng và trở thành gốc rễ của DELTA.

Việc xác minh chỉ đi được đến đó. Trong nhóm tài liệu được đối chiếu ở đây, không có nguồn sơ cấp nào ghi lại giai đoạn ban đầu ấy đến mức có ngày tháng và tên người; hồ sơ công khai dừng lại tại đó. Vì vậy, xưởng làm việc của Aerorozvidka và khung cảnh cuộc gặp đầu tiên không được dựng lại ở đây. Không có tài liệu công khai nào cho biết ai đã nói gì vào đêm nào. Điều có thể xác nhận chỉ là hướng phát triển của dòng gốc. DELTA không giống một thứ sinh ra từ bản kế hoạch của một bộ, mà giống một công cụ do những người cảm thấy nhu cầu sát với chiến sự tạo ra, rồi công cụ ấy đi lên trên và trở thành một hệ thống quốc gia.

Nếu nhầm lẫn ai đã làm việc gì, toàn bộ dòng phát triển sẽ bị bẻ cong. Việc phát triển và vận hành DELTA thuộc về các tổ chức nằm trong quỹ đạo của bộ quốc phòng, còn việc Fedorov ban hành mệnh lệnh đối với DELTA là chuyện của năm 2026. Đọc DELTA như "ứng dụng chiến trường do bộ trưởng kỹ thuật số xây dựng" là một lỗi phổ biến, và bài viết càng ưu ái ông ấy thì càng hay mắc lỗi đó.

Khoảnh khắc DELTA thu hút sự chú ý quốc tế là tin tức về một bài kiểm tra đã vượt qua. Ngày 17 tháng 7 năm 2024, bộ quốc phòng Ukraine thông báo rằng DELTA đã vượt qua một cuộc kiểm toán của NATO.

Nói một hệ thống vượt qua kiểm toán của NATO nghĩa là gì? Để quân đội của nhiều nước có thể chiến đấu cùng nhau, mọi thứ từ tần số vô tuyến, quy ước tọa độ bản đồ cho đến định dạng dữ liệu của thông tin nhắm mục tiêu đều phải đọc được đối với mọi bên. Nếu một tọa độ do một bên gửi đi lại được hệ thống của bên kia hiểu thành một thứ hoàn toàn khác, kết quả không phải là phối hợp mà là tai nạn bắn nhầm quân mình. Khả năng tương thích này được gọi là khả năng tương tác. Kiểm toán của NATO là thủ tục kiểm tra xem một hệ thống có thể trao đổi thông tin theo các chuẩn của NATO hay không, và vượt qua kiểm toán nghĩa là, nói gần đúng, DELTA đã có hình thức có thể đưa vào một bức tranh chỉ huy và kiểm soát kiểu NATO. Với

Ukraine, thông báo ấy vừa là tin kỹ thuật vừa là tin chính trị. Đó là lời tuyên bố rằng hệ thống của chúng tôi nói cùng một ngôn ngữ với phương Tây.

Thành tựu ấy và những giới hạn của nó cần được nhìn cùng lúc.

Bên đưa ra thông báo là Bộ Quốc phòng Ukraine. Hiện không có báo cáo xác minh riêng do NATO ban hành trong hồ sơ công khai. Không có lý do gì để gắn nhãn thông báo của một chính phủ thời chiến là sai ngay từ bề mặt. Nhưng một văn bản trong đó một cơ quan báo cáo thành công của chính mình không thể được cân nhắc ngang với một văn bản đã được một tổ chức bên ngoài xác minh độc lập. Một phần đáng kể các sự kiện đã được xác lập về DELTA dựa trên các thông báo của bộ, và hoàn cảnh đó sẽ không được che giấu ở đây. Xin hãy để mắt tới phần quy nguồn ở cuối các câu. Một câu phát ra từ miệng ai, ở đây, cũng quan trọng không kém nội dung câu đó nói gì.

Vượt qua một tiêu chuẩn và vận hành trong chiến đấu cũng là hai việc khác nhau. Một cuộc kiểm toán xem xét hình thức có đúng hay không. Có bao nhiêu lữ đoàn dùng DELTA ở tiền tuyến, dùng thường xuyên đến mức nào, và chính xác ra sao, những điều đó không được ghi vào báo cáo kiểm toán. Nói theo ngôn ngữ ô tô, nó tương đương với phê duyệt kiểu loại, một việc khác với hồ sơ lái xe trên đường xấu.

Đây là điều cần nhớ về dòng phát triển của DELTA. DELTA là một lớp tích lũy đã đi qua nhiều bàn tay. Có một tường thuật được tiếp nhận rằng nó bắt đầu từ một nhóm kỹ sư tình nguyện; các tổ chức thuộc Bộ Quốc phòng tiếp quản việc phát triển và vận hành; nó được trình bày như một hệ thống chiến đấu cho toàn bộ lực lượng phòng vệ; và vào tháng 7 năm 2024, một thông báo của bộ về việc vượt qua kiểm toán NATO được gắn với nó. Trên lớp tích lũy đó, bộ trưởng quốc phòng mới của năm 2026 đặt chữ ký riêng của mình, và chỉ khi nhìn vào dòng phát triển trước, người ta mới tránh được việc phóng đại hoặc thu nhỏ kích thước của chữ ký ấy.

Để một bản đồ như DELTA có giá trị sử dụng, phải có những con người ở tầng dưới xây dựng các cỗ máy gửi dữ liệu lên bản đồ đó. Khung mà Ukraine dùng để gắn kết tầng dưới ấy là một cụm công nghệ quốc phòng có tên Brave1. Khoảng 2.500 startup và công ty thuộc cụm này, đã đăng ký hơn 5.000 sản phẩm, trong đó có hơn 500 nhà sản xuất thiết bị bay không người lái, hơn 200 nhà sản xuất phương tiện mặt đất không người lái, và hơn 200 nhà sản xuất sản phẩm trí tuệ nhân tạo. Các sản phẩm được nộp lên sẽ được đại diện lực lượng quốc phòng Ukraine xem xét. Họ chọn ra những thứ thật sự cần ở tiền tuyến, rồi kết nối chúng với thử nghiệm thực địa và mã hóa theo chuẩn NATO.

Mã hóa theo chuẩn NATO là thủ tục gắn cho một thiết bị mã số chung và dữ liệu đặc tả mà NATO dùng, để hệ thống cung ứng quân sự của các nước khác nhận ra đó là cùng một đối tượng. Nó đi theo hướng gần giống cuộc kiểm toán NATO mà DELTA đã vượt qua, nhưng là một cánh cửa khác. Một cánh cửa làm cho định dạng trao đổi thông tin khớp nhau; cánh cửa kia làm cho nhãn trên chính đối tượng khớp nhau.

Cần đặt một lưu ý ở đây, một cách có chủ ý. Brave1 không phải là tổ chức xây dựng DELTA. Việc phát triển và vận hành DELTA do các tổ chức thuộc bộ quốc phòng xử lý, và trong nhóm tài liệu được đối chiếu ở đây, hồ sơ công khai chưa cho thấy các cỗ máy của những công ty được Brave1 nuôi dưỡng đưa dữ liệu lên bản đồ mang tên DELTA như thế nào, hoặc loại giấy tờ định chế nào buộc hai trục này lại với nhau. Điều có thể gắn vào dòng phát triển này là sự thật rằng hai dòng chảy ấy lớn lên cạnh nhau, và với những tài liệu hiện có, không thể nói xa hơn thế.

2. Sự thành lập Lực lượng Hệ thống Không người lái và việc định chế hóa drone

Nếu DELTA là công việc gom những con mắt rải rác về thành một, thì trong cùng giai đoạn đó, quân đội Ukraine cũng đang tổ chức lại chính bàn tay cầm chiếc drone.

Quân đội có một khái niệm gọi là quân chủng. Nó chỉ một nhóm quân sự lớn có cơ cấu riêng, chuỗi chỉ huy riêng, ngân sách riêng và học thuyết riêng, như lục quân, hải quân, không quân. Khi một loại vũ khí trở thành quân chủng, điều đó có nghĩa nó trở thành một tổ chức tuyển quân, huấn luyện và viết học thuyết dưới tên của chính mình. Nó có dòng ngân sách riêng trong bảng chi tiêu, có nấc thang thăng tiến riêng, và có một tư lệnh phải chịu trách nhiệm khi thất bại. Ukraine đã trao cho drone vị thế đó, và quân chủng được tạo ra từ đó mang tên Unmanned Systems Forces (USF).

Ngày thành lập được ghi khác nhau tùy từng nguồn. Một báo cáo nói chính phủ Ukraine chính thức thành lập Unmanned Systems Forces vào đầu năm 2024. Một tài liệu khác viết rằng tính đến ngày 16 September 2024, Unmanned Systems Forces đã được tách ra và nâng lên thành một quân chủng độc lập của lực lượng vũ trang Ukraine. Có vẻ đây là khoảng cách giữa tuyên bố và việc hoàn tất cơ cấu, nhưng thay vì đóng đinh vào một ngày duy nhất, nên đặt cả hai mốc cạnh nhau. Một quân chủng mới không ra đời theo cách người ta cắt một chiếc bánh sinh nhật, và cách đọc nó như một quá trình trải dài suốt năm 2024 phù hợp hơn với các tài liệu công khai.

Ở đây có một câu hỏi nằm ngoài hồ sơ công khai. Việc thành lập Unmanned Systems Forces diễn ra rất lâu trước khi Fedorov trở thành bộ trưởng quốc phòng. Ông tiếp quản bộ này vào January 2026. Khá nhiều bản tường thuật, ở Ukraine và nước ngoài, ghi quyết định biến drone thành một quân chủng vào cột thành tích của ông, nhưng tài liệu không ủng hộ điều đó. Đây là cám dỗ cần canh chừng kỹ nhất khi viết về một cuộc đời. Cám dỗ ấy là sắp xếp những việc vốn đã vận hành trước khi nhân vật chính xuất hiện như thể ông đã mang chúng đến cùng mình.

Vị thế của Lực lượng Hệ thống Không người lái thể hiện ngay trong sơ đồ tổ chức. Binh chủng này được đặt ngang hàng với Lực lượng Tác chiến Đặc biệt và Lực lượng Phòng vệ Lãnh thổ. Đại tá Vadym Sukharevskyi được bổ nhiệm làm tư lệnh đầu tiên, và khi trở thành tư lệnh Lực lượng Hệ thống Không người lái, ông đồng thời giữ chức phó cho tổng tư lệnh Oleksandr Syrskyi.

Việc một tư lệnh nắm một chức vụ trực tiếp bên dưới tổng tư lệnh có nghĩa là vấn đề drone đã được chuyển từ cuối danh sách nghị sự của bộ tổng tham mưu vào giữa nhóm chỉ huy. Trong một tổ chức, một việc thường trở nên quan trọng theo cách như vậy. Chỗ ngồi thay đổi trước khẩu hiệu. Khi đã xác định ai ngồi ở đâu trong phòng họp và ai có thể báo cáo trực tiếp với tổng tư lệnh, lĩnh vực đó thực sự có quyền lực. Sơ đồ tổ chức là một văn bản cho thấy, không cần nói một lời, tổ chức ấy coi điều gì là quan trọng.

Khi một binh chủng đã tồn tại, hình dạng các đơn vị của nó cũng thay đổi. Năm 2025, Trung đoàn 14 hiện có được mở rộng và tổ chức lại thành Trung tâm 1 trực thuộc Lực lượng Hệ thống Không người lái. Việc đi từ trung đoàn lên trung tâm không chỉ là thay một tấm biển. Borys, một sĩ quan có liên hệ với đơn vị này, giải thích đó là một lựa chọn chiến lược có chủ ý và nói như sau: "Mục tiêu của chúng tôi không phải là chiến đấu lâu hơn, mà là chiến đấu thông minh hơn. Thông qua độ chính xác, cấu trúc và tư duy kỹ thuật, chúng tôi có thể làm kẻ địch kiệt sức nhanh hơn tốc độ kẻ địch thích nghi."

Một trung đoàn chiến đấu. Một trung tâm vừa chiến đấu, vừa thử nghiệm, giảng dạy và sửa đổi học thuyết. Theo cùng báo cáo đó, Trung tâm 1 được thiết kế như một đầu mối tích hợp, gắn hoạt động tác chiến với thử nghiệm, huấn luyện và cải tiến học thuyết, đồng thời được giao vai trò làm kênh đưa các phát minh ở tiền tuyến vào thực hành để toàn bộ binh chủng có thể dùng. Giả sử một tiểu đoàn tìm ra một mẹo để né gây nhiễu của đối phương. Nếu mẹo đó chỉ nằm trong các cuộc trao đổi vô tuyến của tiểu đoàn, nó sẽ không bao giờ trở thành tài sản của quân đội. Trung tâm là tổ chức biến nó thành tài liệu, đưa nó vào khóa huấn luyện, và mang nó sang đơn vị bên cạnh. Kiến thức từ tiền tuyến chỉ lan rộng khi có người ở đó để mang nó đi.

Cùng báo cáo đó nói rằng 1st Center tự sản xuất 80 đến 90 phần trăm số drone mà đơn vị này dùng trong các chiến dịch ngay bên trong Ukraine, và có khả năng tấn công mục tiêu sâu tới 1.000 km trong lãnh thổ Nga. Những con số này dựa trên phát biểu của đơn vị và những người có liên quan đến đơn vị đó; trong các tài liệu có thể tiếp cận, không có kiểm chứng độc lập chéo. Các con số được giữ lại, nhưng chưa được xác nhận. Bảng thành tích thời chiến do một đơn vị tự công bố, ngay cả khi đúng, cũng không thể được xếp cùng cột với một sự kiện đã được kiểm chứng.

Vai trò của chính các đơn vị drone cũng thay đổi trong giai đoạn này. Một nghiên cứu đánh giá rằng các đơn vị hệ thống không người lái đã vượt ra ngoài vai trò trinh sát phụ trợ cũ và phát triển thành lực lượng hỗ trợ tác chiến đa miền, trải qua trên không, trên bộ và trên biển, trở thành một thành phần cấu trúc của chiến tranh hiệp đồng binh chủng hiện đại. Cách diễn đạt này khá nặng, nên cần tháo ra cho rõ. Drone trước đây là con mắt giúp bộ binh nhìn thấy những gì bộ binh không thể thấy. Drone ngày nay vừa là con mắt, vừa là bàn tay, và nó không còn chỉ ở trên bầu trời.

Sự thay đổi trên biển thường được viện dẫn như bằng chứng. Trong suốt 2024 và 2025, quân đội Ukraine đã đạt tới mức có thể cùng lúc điều hành hàng chục xuồng drone hải quân với các chức năng khác nhau. Xuồng drone hải quân là một tàu nhỏ không có thủy thủ đoàn và được điều khiển từ xa. Đến giai đoạn này, hoạt động drone hải quân đã vượt khỏi kiểu tấn công tự sát lao vào một mục tiêu riêng lẻ, chuyển thành các đòn đánh nhiều hướng kết hợp máy bay không người lái, drone dưới nước, tên lửa hành trình và năng lực tác chiến điện tử. Đã có những trường hợp được ghi nhận về việc gắn tháp pháo hoặc tên lửa cỡ nhỏ trên xuồng, thậm chí có cả trường hợp một xuồng được dùng làm bệ phóng cho một hệ thống chống drone thuộc Special Operations Forces.

Đó là một cấu trúc trong đó một drone chở một drone ra ngoài để bắt một drone. Những tổ hợp như vậy không thể tự ghép lại chỉ bằng một ý tưởng. Phải định trước đơn vị nào lái xuồng, đơn vị nào điều khiển chiếc drone đặt trên xuồng, và phán đoán của ai sẽ được ưu tiên khi liên lạc bị mất. Nội dung thực chất của việc nói rằng một quân chủng đã được lập ra nằm ở đây: đã xác định ai chịu trách nhiệm thiết kế những tổ hợp như vậy, và chỉ khi có người chịu trách nhiệm thì một thành công riêng lẻ mới cứng lại thành một hoạt động có thể lặp lại.

Nhận định rằng drone đã trở thành đặc điểm chi phối của chiến tranh hiện đại cũng được lặp lại bởi các cơ sở nghiên cứu quân sự bên ngoài Ukraine. Đây là một chẩn đoán vẫn đứng vững ngay cả khi gạt bỏ các tuyên bố của chính phủ Ukraine, và nền tảng của nó tương đối dày dặn.

Nhưng thể chế hóa không đồng nghĩa với chiến thắng. Những cảnh báo mà báo cáo được dẫn để lại được ghi nguyên trạng ở đây.

Một vấn đề là sự trôi dạt về tổ chức. Báo cáo về Unmanned Systems Forces nêu sự trôi dạt thể chế là nỗi lo lớn của binh chủng này khi bước vào năm 2026, và nói thẳng rằng 1st Center không được tách khỏi thực tế chiến đấu. Khi một đơn vị đổi mới trở thành một thiết chế, giấy tờ và cuộc họp tăng lên, và cái bẫy mất cảm giác về tiền tuyến mở ra. Câu chuyện những người nổi dậy của hôm qua trở thành các quan chức bàn giấy của hôm nay cũng đủ quen thuộc ngoài quân đội.

Vấn đề còn lại là chẩn đoán về phần còn thiếu. Cùng báo cáo đó định nghĩa nhiệm vụ trước mắt của họ là chuyển đổi thành một bộ chỉ huy mở rộng, có khả năng tạo ra hiệu ứng chiến lược bền vững trên toàn chiến trường, và không đưa các thiếu hụt công nghệ cũng như việc tạo năng lực xuất kích vào danh sách ấy. Những điều kiện mà báo cáo nêu là chỉ huy và kiểm soát, đánh giá thiệt hại sau trận đánh, và năng lực thử nghiệm liên tục. Đánh giá thiệt hại sau trận đánh là quy trình xác nhận sau một đòn tấn công rằng thực tế đã phá hủy được gì và mức độ bao nhiêu, rồi đưa kết quả đó vào quyết định tiếp theo. Trọng tâm đã chuyển từ bài toán chế tạo thật nhiều drone sang bài toán chỉ huy thông tin và các đòn đánh do drone tạo ra, và khoảng trống nơi DELTA và Mission Control đứng chính là vai trò chỉ huy và kiểm soát, đánh giá thiệt hại sau trận đánh, và thử nghiệm ấy.

Trang bị mà binh chủng mới sẽ sử dụng đến từ các công ty tư nhân và hệ thống mua sắm nhà nước. Ngày 28 April 2025, Ukraine mở một chợ trực tuyến mang tên Brave1 Market. Đây là kênh đưa nhanh ra tiền tuyến những thiết bị như khí tài tác chiến điện tử tầm ngắn, drone đánh chặn để ngăn drone đối phương, drone gắn AI và drone cáp quang. Drone cáp quang trao đổi tín hiệu qua một sợi thủy tinh mảnh như sợi tóc, được nhả ra phía sau nó thay vì dùng sóng vô tuyến. Vì đường truyền được nối vật lý, quyền điều khiển không bị mất ngay cả khi đối phương áp chế phổ vô tuyến.

Chợ này vận hành như sau. Khi một đơn vị tiền tuyến tấn công đối phương và xác nhận khoảnh khắc đó bằng video, đơn vị ấy nhận điểm chiến đấu theo các hệ số mà chính phủ đã đặt trước. Thay vì chờ giấy phê duyệt từ bộ hoặc bộ tổng tham mưu, đơn vị dùng số điểm đó để đặt trực tiếp từ nhà sản xuất loại drone có đúng thông số họ cần ngay lúc này. Khi hợp đồng được ký, bộ trả tiền mặt cho nhà sản xuất.

Trong quá trình này, yêu cầu của quân đội và lợi ích của các công ty va vào nhau. Lý do mà các tài liệu đưa ra cho việc thành lập Unmanned Systems Forces là nhu cầu gom việc triển khai tác chiến của các đơn vị drone rải rác về một đầu mối. Trái lại, chợ trực tuyến lại đẩy quyền mua sắm xuống các đơn vị. Hồ sơ công khai dừng lại trước bất kỳ tài liệu nào giải thích cách dung hòa lực kéo lên trên và lực thả xuống dưới ấy, hoặc bộ tư lệnh binh chủng can dự tới đâu vào đơn đặt hàng của từng đơn vị. Ai đặt ra và sửa các hệ số quyết định một mục tiêu nhất định đáng bao nhiêu điểm, và liệu một đơn vị có thể phản đối phán quyết xác nhận hay không, cũng là những nơi hồ sơ công khai dừng lại.

Tiền từ bên ngoài cũng đi vào đúng vị trí trong giai đoạn này. Ngày 22 July 2025, Ukraine và European Union khởi động một liên minh công nghệ quốc phòng trị giá 100 million euros. Theo phía EU, BraveTech EU, chương trình gắn với liên minh này, là một cơ chế buộc European Defence Fund, EU Defence Innovation Scheme và Brave1 vào một khung duy nhất cho phát triển, thử nghiệm và triển khai chung. Lý do được nêu là đưa tri thức mà Ukraine giành được trên chiến trường quay trở lại châu Âu. Cơ quan công bố là European Commission, chi tiết ấy được ghi nhận ở đây.

3. Mission Control, nhắm mục tiêu bằng AI, và việc nối phản hồi từ chiến trường

Giả sử drone của nhiều đơn vị cùng bay trên một khoảng trời. Trong lúc máy bay trinh sát của Tiểu đoàn A phát hiện một mục tiêu và báo cáo, drone tấn công của Lữ đoàn B bay về phía cùng mục tiêu đó. Đơn vị C, không biết gì về việc này, đưa drone của mình lên cùng vùng trời. Chỉ có một mục tiêu, nhưng ba phương tiện bị dồn vào đó, không phận trở nên rối, và thiết bị tác chiến điện tử của phía mình rốt cuộc chặn luôn liên lạc của drone phía mình cùng với mọi thứ khác.

Khi drone còn hiếm, tình trạng ùn tắc này chưa xuất hiện. Drone càng nhiều, giá càng rẻ, và mỗi lữ đoàn càng tự vận hành đội drone riêng, tình trạng ùn tắc càng nặng. Vấn đề do thành công tạo ra quay lại thành một gánh nặng mới. Chỉ huy và kiểm soát là chức năng sắp xếp tại một nơi rằng ai làm gì, vào lúc nào và ở đâu. Mission Control, hệ thống mà sắc lệnh do Fedorov ký ngày 23 tháng 1 năm 2026 yêu cầu đưa vào vận hành, là một thiết kế để làm việc sắp xếp đó trên nền bản đồ hiện có mang tên DELTA. Thay vì vẽ thêm một bản đồ nữa, nó đặt một lớp mới lên bản đồ đã có sẵn.

Tài liệu công khai về việc này không nhiều. Về Mission Control, tài liệu công khai chỉ gồm một thông báo duy nhất của Bộ Quốc phòng Ukraine. Có thể xác nhận được rằng sắc lệnh đã được ký, rằng hệ thống xử lý chỉ huy và kiểm soát drone bên trong DELTA, và ngày ký là 23 tháng 1 năm 2026. Phạm vi xác nhận chỉ đến đó. Hệ thống thực tế được triển khai tới bao nhiêu đơn vị, mức trùng lặp mục tiêu giảm bao nhiêu ở nơi nó được triển khai, và kết quả chiến đấu thay đổi ra sao: hồ sơ công khai dừng lại tại đó. Một chữ ký vào ngày thứ chín sau khi nhậm chức có ý nghĩa biểu tượng lớn, nhưng biểu tượng không thể được chép lại như một kết quả. Lý do chữ ký đó mở ra chương này là vì nó cho thấy vị bộ trưởng mới đã đặt tay vào đâu.

Trong cùng giai đoạn này, DELTA cũng đi xuống tới tay từng người lính. Ngày 10 March 2026, Bộ Quốc phòng Ukraine thông báo rằng binh sĩ sẽ nhận cảnh báo về mối đe dọa trên không thông qua ứng dụng DELTA Mobile. Tại thời điểm thông báo, đây là một kế hoạch được nêu ra, còn việc triển khai thực tế đã đi xa đến đâu thì hồ sơ công khai dừng lại ở đó. Chỉ riêng hướng đi đã rất rõ. Thông tin theo dõi trước đây xuất hiện trên màn hình lớn gắn trên tường sở chỉ huy sẽ được đẩy xuống thiết bị cá nhân trong chiến hào và trên các xe đang di chuyển.

Trong quân đội, còn một vấn đề nữa gắn với việc này. Liên lạc ở tiền tuyến thường xuyên bị gián đoạn, và tác chiến điện tử của đối phương luôn săn tìm tín hiệu. Một thiết kế đẩy thông tin xuống thiết bị cá nhân sẽ chịu đựng được môi trường ấy tốt đến đâu là điều thông báo không trả lời.

Các thông báo của chính bộ này ghi lại cả những thành tựu lẫn những việc còn bỏ ngỏ. Ngày 2 February 2026, bộ công bố bản tóm tắt về các khóa huấn luyện mà binh sĩ đang học trong ứng dụng Army+. Việc các khóa liên quan đến drone đứng đầu, trong khi DELTA vẫn là vấn đề chưa giải quyết xong, vừa là tiêu đề vừa là nội dung chính của thông báo đó.

Xây dựng một hệ thống và khiến con người dùng nó là hai việc khác nhau. Một hệ thống tác chiến đã vượt qua kiểm tra của NATO, kể cả sau khi binh chủng được chính thức thành lập, vẫn tụt lại trong danh sách học tập của chính những người lính lẽ ra phải xử lý nó hằng ngày. Có một khoảng cách giữa danh sách tính năng trong các tài liệu giới thiệu DELTA và màn hình mà một tiểu đội trưởng ở tiền tuyến thực sự bật lên để dùng. Cần ghi lại rằng cơ quan công bố sự thật này chính là Bộ Quốc phòng Ukraine. Một thông báo trong đó một cơ quan tự viết ra điểm yếu của mình là điều hiếm thấy trong các tài liệu của một chính phủ thời chiến.

Thu hẹp khoảng cách ấy là nhiệm vụ mà Fedorov phải đối mặt tại bộ. Với một dịch vụ dân sự, nếu mức sử dụng thấp thì người ta sửa giao diện và mua quảng cáo. Trong quân đội, việc một hệ thống ít được dùng là vấn đề trong đó mệnh lệnh, huấn luyện, điều kiện liên lạc và niềm tin của binh sĩ cùng lúc rối vào nhau. Một tiểu đội trưởng không bật ứng dụng thường có lý do. Pin yếu, hoặc không có tín hiệu, hoặc vài giây nhìn vào màn hình là nguy hiểm, hoặc từng có ký ức tin vào màn hình ấy một lần rồi gặp nạn. Số liệu sử dụng không cho biết lý do.

Những điều có thể nói về AI trong chỉ thị mục tiêu là rất hẹp. Có phân tích cho rằng trên chiến trường Ukraine đang xuất hiện xu hướng tiến tới tự chủ, trong đó drone tự tìm đường đến mục tiêu ngay cả khi tín hiệu định vị vệ tinh bị cắt, và nhiều máy bay phối hợp thành bầy. Môi trường bị cắt định vị vệ tinh nghĩa là trạng thái trong đó đối phương đã áp chế phổ điện từ khiến tọa độ GPS không thể được tiếp nhận. Việc các hồ sơ chiến trường mà DELTA tích lũy trở thành vật liệu cho dạng tự động hóa như vậy, xét về cấu trúc, cũng là một nhận định có thể hiểu được.

Nhưng thuật toán nào xử lý mục tiêu nào, ở mức tự chủ nào, và sự phê chuẩn của con người can thiệp ở giai đoạn nào, thì chưa có tài liệu gốc đã được xác nhận. Câu hỏi ai chịu trách nhiệm khi nhận dạng mục tiêu sai cũng vẫn bỏ ngỏ. Khi không có tài liệu, viết rõ rằng không có tài liệu là thành thật với người đọc hơn so với việc lấp chỗ trống bằng tưởng tượng.

Tổ chức, trang bị và hệ thống thông tin của lực lượng không người lái vận động gắn chặt với nhau. DELTA là một công cụ đi từ dưới lên. Có một cách kể được tiếp nhận rộng rãi rằng nó bắt đầu trong tay các tình nguyện viên và kỹ sư; các tổ chức thuộc bộ quốc phòng tiếp quản việc phát triển và vận hành; và vào tháng 7 năm 2024, một thông báo của bộ về việc vượt qua cuộc kiểm toán NATO được gắn với nó. Các hệ thống không người lái đã đi từ trang bị thành một quân chủng. Trong năm 2024, Unmanned Systems Forces được thành lập, tư lệnh lực lượng này kiêm cấp phó của tổng tư lệnh, và đến năm 2025, 14th Regiment được tổ chức lại thành 1st Center, tạo ra một tổ chức vừa chiến đấu vừa học. Cả hai dòng chuyển động này đều đã lớn lên trước khi Fedorov trở thành bộ trưởng quốc phòng.

Điều ông làm là ký một văn bản đặt lên trên chúng một lớp chỉ huy và kiểm soát. Chỉ dựa vào các tài liệu của nửa đầu năm 2026 thì chưa thể nói chữ ký đó có làm thay đổi tiền tuyến hay không. Điều rõ ràng là hệ thống mà ông tiếp nhận vốn đã gặp vấn đề ngay với chính tên gọi của nó. Một bên là chẩn đoán của chính bộ này rằng DELTA đang chậm trong các danh sách huấn luyện binh sĩ; bên kia là chẩn đoán trong báo cáo, nêu chỉ huy và kiểm soát cùng đánh giá thiệt hại chiến đấu là nhiệm vụ tiếp theo của Unmanned Systems Forces. Cả hai cùng chỉ về một nơi. Công cụ đã có; cách dùng các công cụ ấy cùng nhau vẫn chưa thật sự được định hình đầy đủ.

Biến drone thành một quân chủng chỉ cần một mệnh lệnh. Làm cho quân chủng ấy thật sự nhìn vào cùng một bản đồ và hành động theo cùng một phán đoán thì cần nhiều mệnh lệnh hơn, và cần nhiều thời gian hơn thế rất xa. Văn bản được ký ngày 23 January 2026 nằm ở điểm khởi đầu của khoảng thời gian đó.

Trong câu chuyện trí tuệ nhân tạo xử lý mục tiêu, công ty duy nhất được các tài liệu nêu tên thật sự là Swarmer. Styx của công ty này là một công nghệ bầy đàn cho phép tối đa 25 drone giữ vị trí đồng bộ với nhau và di chuyển cùng nhau ngay cả ở nơi tín hiệu định vị vệ tinh bị cắt. Con đường của công ty này tới các khoản tài trợ và đầu tư đã được mô tả ở Chapter 7, trong hệ sinh thái công nghiệp Brave1. Điều cần giữ lại ở đây là không có bằng chứng nào cho thấy công nghệ đó được liên kết với DELTA hoặc Mission Control.

Mối liên hệ với Mission Control cũng vẫn để ngỏ. Có phân tích cho rằng trên chiến trường đang xuất hiện một xu hướng: drone tự tìm mục tiêu ở nơi định vị vệ tinh bị chặn, còn nhiều phi cơ di chuyển cùng nhau theo bầy. Nhưng về việc công nghệ bầy đàn của Swarmer trên thực tế có được liên kết với DELTA hoặc Mission Control hay không, và con người xác nhận một mục tiêu do bầy drone chọn ở giai đoạn nào, hồ sơ công khai dừng lại tại đó. Khoảng cách giữa bức tranh có thể suy ra từ cấu trúc và bức tranh được tài liệu xác nhận được để nguyên tại đây, chưa khép lại.

Chương 9. Từ Bộ trưởng Kỹ thuật số đến Bộ trưởng Quốc phòng

1. Tháng 1 năm 2026: Đề cử của Zelensky và cuộc bỏ phiếu tại quốc hội

Trong cơ sở dữ liệu lập pháp của Verkhovna Rada Ukraine có một văn bản duy nhất ghi ngày 14 tháng 1 năm 2026. Verkhovna Rada là quốc hội Ukraine. Văn bản này là một nghị quyết, mang số 4756-IX, với nhan đề: "Về việc bổ nhiệm Mykhailo Albertovych Fedorov làm Bộ trưởng Quốc phòng Ukraine." Nội dung của nó ngắn gọn. Tổng thống đưa ra đề cử, quốc hội bỏ phiếu, việc bổ nhiệm được xác nhận. Một hồ sơ thủ tục, không hơn.

Dấu vết chính thức còn lại từ thời điểm người mà chúng ta đang theo dõi bước vào Bộ Quốc phòng chỉ dài một trang. Bài đăng trên mạng xã hội cầu cứu internet vệ tinh không nằm trên trang đó. Dây chuyền lắp ráp của một nhà máy drone cũng không có ở đó, cũng như gian trình diễn tại một triển lãm startup. Khi một nhà nước trao quyền cho một người, thứ nó để lại là một tờ giấy duy nhất có đánh số, và bất kỳ ai viết về một cuộc đời đều phải bắt đầu từ tờ giấy đó, không tô vẽ những điều tờ giấy không nói như thể tờ giấy đã nói ra.

Ở Ukraine, tổng thống không thể tự mình bổ nhiệm bộ trưởng quốc phòng. Tổng thống đưa một ứng viên ra trước quốc hội, và quốc hội phải phê chuẩn bằng bỏ phiếu thì việc bổ nhiệm mới hoàn tất. Vì vậy, các cuộc bổ nhiệm bộ trưởng luôn để lại hai hồ sơ: đề cử từ phía tổng thống và nghị quyết từ phía quốc hội. Trong trường hợp của Fedorov, hai hồ sơ đó chỉ cách nhau một ngày.

Quá trình này bắt đầu bằng việc tổng thống công khai đề cử nhân sự. Ngày 13 January 2026, Tổng thống Volodymyr Zelensky đăng một bài phát biểu trên website chính thức của Văn phòng Tổng thống. Bài này có nhan đề "Today We Have Begun a Genuine Reboot," với phụ đề mô tả những thay đổi nội bộ nhằm giúp Ukraine vững hơn. Về hình thức, đó là một bài phát biểu, nhưng từng dòng lại dày đặc tên người và chức vụ, khiến văn bản này gần với một thông báo nhân sự hơn.

Bài phát biểu nêu kế hoạch sắp xếp lại bộ máy quốc phòng. Kyrylo Budanov, người từng lãnh đạo tổng cục tình báo quân sự, sẽ đảm nhiệm vị trí Chánh Văn phòng Tổng thống. Tổng cục tình báo quân sự thuộc Bộ Quốc phòng và có nhiệm vụ phát hiện các hoạt động của đối phương; tại Ukraine, cơ quan này thường được gọi bằng chữ viết tắt HUR. Chức vụ Budanov để lại sẽ được giao cho Oleh Ivashchenko, người đang điều hành cơ quan tình báo đối ngoại. Bài phát biểu cũng công bố các thay đổi trong cơ cấu chỉ huy và lãnh đạo của lực lượng biên phòng, cùng lời hứa gửi tới quốc hội một dự luật cải tổ State Bureau of Investigation, cơ quan điều tra tội phạm do quan chức cấp cao và các cơ quan thực thi pháp luật gây ra. Văn bản còn nhắc đến một biện pháp đưa một phó chánh Văn phòng Tổng thống có kinh nghiệm chỉ huy chiến đấu vào liên lạc trực tiếp với các lữ đoàn.

Việc tái cơ cấu Bộ Quốc phòng là một phần trong kế hoạch đó. Tổng thống nói ông sẽ thay đổi "format of work" của bộ, và cho biết ông đã đề nghị Mykhailo Fedorov giữ chức bộ trưởng quốc phòng. Ông nói thêm rằng bộ trưởng quốc phòng sắp rời nhiệm sở, Denys Shmyhal, sẽ vẫn ở trong đội ngũ và đảm nhận các nhiệm vụ nhà nước khác.

Bài phát biểu này là một văn bản do Văn phòng Tổng thống ban hành về chính mình. Một văn bản trong đó chính phủ giải thích các quyết định nhân sự của mình có thể xác nhận sự kiện về các quyết định ấy. Ai được đề cử, vào thời điểm nào, và vào chức vụ nào, những điểm đó được văn bản này xác lập. Nhưng cùng văn bản ấy không xác nhận được phần đánh giá gắn với các quyết định đó. Từ "reboot" trong bài phát biểu là cách chính phủ tự đóng khung câu chuyện, và nó nằm ở một tầng khác với chẩn đoán của một cơ quan độc lập. Không chính phủ nào gọi cuộc thay máu nhân sự của mình là xử lý thiệt hại; họ luôn gọi đó là một bước tiến. Vì vậy, cần đọc tách hai tầng này. Ngày tháng, tên người và chức danh được văn bản cố định; vì sao các bổ nhiệm này trở nên cần thiết vẫn là vấn đề diễn giải.

Ngày hôm sau, 14 tháng 1, quốc hội bỏ phiếu. Cùng ngày, Bộ Quốc phòng Ukraine phát hành thông cáo báo chí bằng tiếng Anh, công bố rằng Fedorov đã được bổ nhiệm làm bộ trưởng quốc phòng mới. Cuộc bỏ phiếu được thông qua với 277 phiếu thuận.

Muốn nói chính xác con số 277 có nghĩa gì, trước hết phải nói rõ nó không có nghĩa gì. Tài liệu được tham khảo chỉ cho biết có 277 phiếu thuận. Bao nhiêu người bỏ phiếu chống, bao nhiêu người bỏ phiếu trắng, bao nhiêu đại biểu hoàn toàn không tham gia bỏ phiếu, hồ sơ công khai dừng lại ở đó. Vì vậy, chỉ riêng con số này không đủ để gắn cho cuộc bỏ phiếu kết luận như "ủng hộ áp đảo" hay "thông qua sít sao". Điều đã được xác nhận là việc bổ nhiệm được thông qua với 277 phiếu thuận, và một con số chỉ bắt đầu lên tiếng khi mẫu số và bối cảnh đi kèm nó cũng được xác nhận.

Hồ sơ còn một khoảng trống nữa. Trước khi Fedorov có thể trở thành bộ trưởng quốc phòng, ông phải rời chức Phó Thủ tướng thứ nhất kiêm Bộ trưởng Chuyển đổi số. Việc từ chức, hoặc bị miễn nhiệm đó, cũng sẽ phải đi qua một thủ tục của quốc hội. Nhưng tài liệu gốc thu được, tức nghị quyết bổ nhiệm, chỉ bao trùm việc bổ nhiệm vào Bộ Quốc phòng. Tài liệu gốc là hồ sơ nguyên thủy do chính các bên trong sự kiện để lại: nghị quyết của quốc hội, bài phát biểu của tổng thống, thông cáo báo chí của một bộ. Không có tài liệu gốc riêng nào cho biết ngày nộp đơn từ chức hoặc số phiếu trong cuộc bỏ phiếu miễn nhiệm để đối chiếu. Các bản tóm tắt thứ cấp trong phạm vi công khai có những câu nói về một lá đơn từ chức được nộp vào đầu tháng 1 và một cuộc miễn nhiệm được thông qua với 270 phiếu. Những thông tin đó hợp lý, và rất có thể là đúng. Nhưng các con số không kiểm tra được nguồn đã không được đưa vào văn bản này. Một khi một con số được đưa vào bản in, nó cứng lại thành thứ trông giống như sự kiện đã được kiểm chứng, rồi tiếp tục đi vào cuốn sách kế tiếp và bài báo sau đó.

Một câu Fedorov nói trong nghị trường đã được nhiều cơ quan truyền thông đăng lại. Về đại ý, ông nói rằng trước cuộc xâm lược toàn diện của Nga, ở Ukraine chưa từng có một công ty tư nhân nào chế tạo tên lửa hoặc robot; nay thì đã có hàng chục công ty như vậy.

Trong phát biểu nhậm chức, Fedorov chỉ ra công việc ông đã làm tại Ministry of Digital Transformation như nền tảng cho cải cách quốc phòng. Ông không đi lên qua các hành lang của Ministry of Defence, và ông chưa từng mặc quân phục. Điều ông có thể đặt trước các đại biểu là hệ mạch mà ông đã xây dựng phía sau ngành công nghiệp quốc phòng trong vài năm qua. Hệ mạch biến tiền quyên góp của công dân thành các hợp đồng drone; hệ mạch đưa nguyên mẫu của một startup ra bãi thử của quân đội; hệ mạch rút thời gian chờ chứng nhận và hợp đồng từ nhiều tháng xuống còn vài tuần. Cầm trong tay những sản phẩm của hệ mạch mà chúng ta đã thấy ông xây dựng, giờ đây ông mở cánh cửa của bộ mua chính những sản phẩm ấy.

Các nhà báo và nhà phân tích nước ngoài đọc việc bổ nhiệm này theo nhiều cách. Một podcast phân tích chính sách phát hành ngày 28 January 2026 mô tả cuộc cải tổ là sự ra mắt của một "war cabinet." Các khách mời trong chương trình lập luận rằng quyền lực đã được tập trung vào tay người đứng đầu Office of the President, Andriy Yermak, và thông tin đến tổng thống đã bị lọc; họ xem việc đưa Budanov và Fedorov lên vị trí mới như một sự phân tán quyền lực.

Cách đọc ấy có sức thuyết phục, nhưng phải được tách khỏi sự thật đã được xác nhận. Những khách mời podcast đó không thể nào tiếp cận biên bản họp của Office of the President. Vì sao tổng thống chọn một quan chức công nghệ thông tin ngoài ba mươi tuổi làm bộ trưởng quốc phòng thời chiến, và các cuộc bàn bạc nội bộ quanh lựa chọn ấy đã diễn ra thế nào, không có tài liệu gốc nào trong số tư liệu thu được cho thấy điều đó. Lý do của Zelensky, những phản đối hay ủng hộ từ các cố vấn của ông, điều Fedorov cân nhắc khi lời đề nghị được đưa ra. Người đọc càng muốn biết nhiều về một đoạn nào đó của câu chuyện, nền đất bên dưới đoạn ấy thường càng mỏng, và cách duy nhất để tránh lấp khoảng nền mỏng ấy bằng trí tưởng tượng là để những khoảng trống vẫn là khoảng trống.

Có thể xác lập được chừng này. Ngày 13 January 2026, tổng thống công khai tuyên bố rằng ông sẽ thay đổi cách làm việc của Ministry of Defence và nêu tên Fedorov; ngày 14 January, quốc hội thông qua resolution 4756-IX với 277 phiếu thuận; và Ministry of Defence công bố chính thức việc này trong cùng ngày.

Những chi tiết khác trong bài phát biểu cũng cho thấy tính chất của cuộc cải tổ. Tổng thống nói rằng Pavlo Palisa, một phó chánh Văn phòng Tổng thống có kinh nghiệm chỉ huy chiến đấu, sẽ trao đổi trực tiếp với các lữ đoàn, và hệ thống giáo dục quân sự sẽ được làm lại để phù hợp với thực tế chiến trường. Về bộ trưởng quốc phòng sắp rời nhiệm sở Denys Shmyhal, ông giải thích rằng Shmyhal sẽ tiếp tục ở lại trong đội ngũ vì đã làm việc có hệ thống, trong đó có việc

chỉ đạo sản xuất hơn một nghìn drone đánh chặn mỗi ngày. Đánh giá ấy và con số ấy là lời của chính tổng thống về chính phủ của ông, và không thể kiểm chứng bằng các thống kê sản xuất riêng biệt.

Những câu chuyện lan truyền bên ngoài về lý do của cuộc cải tổ cụ thể hơn nhiều. Các khách mời trong podcast cuối tháng Một đó nói rằng Andriy Yermak, chánh Văn phòng Tổng thống, không chỉ nắm các đòn bẩy quyền lực mà còn lọc thông tin đến tận tổng thống, và vì tin xấu bị chặn lại nên tình trạng thật của việc tuyển quân và khủng hoảng năng lượng chỉ được biết đến muộn. Chương trình ấy cũng nói rằng chỉ sau cuộc gặp với Tổng thống Trump ở Florida, Zelensky mới đối diện với mức độ nghiêm trọng của tình hình. Còn có một nhận định về việc các vụ án tham nhũng trùng thời điểm với những nỗ lực nhằm làm suy yếu các cơ quan chống tham nhũng.

Mỗi tường thuật như vậy đều giả định rằng người kể biết điều gì đã xảy ra bên trong Văn phòng Tổng thống. Nhưng không có cơ sở để nói rằng những người xuất hiện trong chương trình có bất kỳ kênh nào để kiểm chứng phần nội bộ ấy. Ngay cả tên gọi "war cabinet" cũng không phải do chính phủ đặt ra; đó là cách các nhà phân tích gọi. Các tài liệu gốc thu được chỉ gồm bài phát biểu của tổng thống, nghị quyết của quốc hội và thông cáo báo chí của Bộ Quốc phòng, và không tài liệu nào có danh sách điểm danh cho thấy các phe đã di chuyển thế nào trong cuộc bỏ phiếu.

2. Một bộ giữa thời chiến, được giao lại cho một người ba mươi lăm tuổi

Các bài viết vào thời điểm ông được bổ nhiệm nêu tuổi của ông khác nhau, khi là ba mươi tư, khi là ba mươi lăm. Có nơi gọi ông là người ba mươi tư tuổi; có nguồn lại gọi ông là ba mươi lăm tuổi. Yonhap News, trong một bài viết đề ngày 21 January 2026, mô tả ông là "bộ trưởng quốc phòng Ukraine 34 tuổi", trong khi một bài đăng trên một cơ quan truyền thông tiếng Anh vào mùa xuân năm 2026, khi bàn về sự trẻ trung của giới lãnh đạo Ukraine, giới thiệu ông là ba mươi lăm tuổi. Không cách nào sai. Sinh nhật của Fedorov là 21 January.

Dù vậy, cũng phải nói rõ rằng ngày sinh này chưa có nền tảng thật chắc. Trong các tài liệu đã được tham khảo, tài liệu duy nhất ghi 21 January 1991 là ngày sinh của ông là mục Wikipedia tiếng Trung. Wikipedia là nguồn bậc ba. Nghĩa là một bản tóm lược được biên soạn bằng cách dẫn lại các nguồn khác, và ở những mục như ngày sinh của một người, lỗi phát sinh trong quá trình biên tập có thể vẫn còn. Vì thế, khi nói về tuổi của ông, cần tách hai tầng khác nhau. Việc ngày bổ nhiệm là 14 January 2026 là sự kiện đã được ấn định bằng một nghị quyết của quốc hội; còn việc ông ba mươi tư tuổi vào ngày đó là phép tính dựa trên một nguồn công khai bậc ba.

Bản thân phép tính thì dễ. Nếu ông sinh ngày 21 January 1991, thì vào ngày 14 January 2026 ông ba mươi tư tuổi, còn thiếu một tuần nữa mới đến sinh nhật thứ ba mươi lăm, và một tuần

sau, vào ngày 21 January, ông bước sang tuổi ba mươi lăm. Bài của Yonhap xuất hiện đúng ngày 21 January ấy, nhưng nêu tuổi của ông là ba mươi tư tính theo thời điểm bổ nhiệm. Nguồn mùa xuân nói ông ba mươi lăm tuổi cũng đúng vì cùng lý do. Khi các con số khác nhau, khác biệt nằm ở ngày được lấy làm mốc, vì vậy cuốn sách này ghi ông ba mươi tư tuổi vào thời điểm bổ nhiệm và ba mươi lăm tuổi ngay sau đó.

Lý do phải xác định tuổi cho chính xác là vì tuổi trẻ của ông thường được nhấn mạnh trong các bài viết về ông. Khi viết về Fedorov, tuổi tác gần như luôn xuất hiện trước, như một phần bổ nghĩa. Vị bộ trưởng trẻ nhất hai mươi tám tuổi; vị bộ trưởng quốc phòng thời chiến ba mươi tư tuổi. Tuổi tác làm câu chuyện trở nên nhanh hơn, nhưng không làm nó chính xác hơn. Ngay khi tuổi được đặt lên trước, người đọc nhìn thấy sự trẻ tuổi của ông thay vì năng lực của ông, rồi lướt qua như thể chính sự trẻ tuổi ấy đã là bằng chứng của cải cách. Điều quan trọng hơn tuổi của ông là tổ chức và những vấn đề mà ông tiếp nhận tại Ministry of Defence.

Ở Ukraine thời chiến, Bộ Quốc phòng là nơi dòng tiền chảy mạnh nhất. Bộ này mua vũ khí, mua đạn pháo, mua thực phẩm và quần áo, rồi trả lương cho hàng trăm nghìn người. Việc một chính phủ mua hàng hóa và dịch vụ như vậy được gọi là mua sắm công. Nơi nào tiền chảy mạnh, nơi đó các vấn đề mua sắm công luôn đi theo. Hợp đồng bị đội giá, hàng tiếp tế không bao giờ được giao, kho bãi chỉ tồn tại trên giấy, đó là những cái bóng đã treo trên bộ này từ lâu.

Podcast phân tích vào tháng 1 năm 2026 đã mô tả Bộ Quốc phòng như một cơ quan bị tàn phá bởi tham nhũng và kém hiệu quả trong mua sắm công, đồng thời chia sứ mệnh của Fedorov thành hai phần: một là chỉnh đốn mua sắm công và quản trị nội bộ; hai là chuyển cách tiến hành chiến tranh sang nền tảng công nghệ. Chẩn đoán này là quan điểm của các nhà phân tích bên ngoài. Nó có sức nặng khác với kết luận của cơ quan kiểm toán hay cáo trạng của công tố viên. Dù vậy, khi chính tổng thống đã nêu riêng cách thức làm việc của bộ này là đối tượng phải thay đổi trong bài phát biểu của mình, ít nhất có thể xác nhận rằng ngay trong nội bộ chính phủ, bộ này cũng được xếp vào nhóm cần sửa chữa. Khi tự chẩn đoán của chính phủ và phê bình từ bên ngoài cùng chỉ về một hướng, khả năng hướng đó là thật sẽ tăng lên, nhưng giữa một khả năng tăng lên và một sự thật đã được xác lập vẫn còn một khoảng cách.

Một số tường thuật về sự nghiệp trước đó của ông bị đưa sai. Thỉnh thoảng vẫn xuất hiện những câu gợi ý rằng Fedorov đã lập ra lực lượng drone sau khi trở thành bộ trưởng quốc phòng, nhưng thứ tự sự kiện thực ra bị đảo ngược.

Unmanned Systems Forces (USF) là một quân chủng riêng của lực lượng vũ trang Ukraine. Quân chủng nghĩa là một trong các bộ phận quân sự lớn như lục quân, hải quân hoặc không quân. Vì vậy, các đơn vị phụ trách drone đã được chính thức nâng lên thành một quân chủng như vậy. Hồ sơ về thời điểm lực lượng này được thành lập khác nhau tùy nguồn. Một báo cáo nghiên cứu ghi rằng lực lượng này được nâng lên thành quân chủng độc lập vào tháng 9 năm 2024, và ghi nhận rằng tư lệnh đầu tiên của lực lượng đồng thời giữ chức cấp phó của tổng tư

lệnh. Một nguồn khác ghi thời điểm thành lập là đầu năm 2024. Thay vì chọn một trong hai, cuốn sách này đặt hai hồ sơ cạnh nhau và trình bày sự khác biệt đúng như một sự khác biệt.

Dù chọn mốc ngày nào, kết luận vẫn như nhau. Những sự kiện này diễn ra hơn một năm trước khi ông được bổ nhiệm làm bộ trưởng quốc phòng. Như đã thấy ở phần trước, hệ thống chiến trường DELTA cũng không phải là một sản phẩm do bộ của ông xây dựng. Dòng phát triển của nó bắt nguồn từ Aerorozvidka, còn trung tâm phát triển và vận hành nằm trong cơ cấu quốc phòng.

Trong thời gian làm Bộ trưởng Chuyển đổi số, ông phụ trách việc mua sắm và sản xuất drone, cũng như việc kết nối các startup với quân đội. Việc lập đơn vị và bổ nhiệm chỉ huy nằm ngoài phạm vi thẩm quyền của ông, và quyền thay đổi biên chế tác chiến của lục quân không nằm trong tay ông. Đến lúc ông chuyển sang Bộ Quốc phòng, hệ thống mua sắm mà ông góp phần định hình đã vận hành rồi. Nếu đảo ngược thứ tự này, hai việc xảy ra cùng lúc: thành tích của ông bị phóng to hơn thực tế, còn phần cải cách được tích lũy qua nhiều năm bên trong quân đội bị xóa đi. Khi một tiểu sử bắt đầu xóa mờ các định chế để làm một con người lớn hơn, nó không còn là tiểu sử nữa mà trở thành một tập quảng bá.

Về hướng đi mà ông chọn ngay sau khi nhậm chức, có một bản tin bằng tiếng Hàn. Yonhap News, trong bài viết ngày 21 January 2026, đưa tin rằng Fedorov đã bắt tay thay thế các drone do Trung Quốc sản xuất, vốn từng gây lo ngại về an ninh, bằng khung thân bay do Ukraine chế tạo, đồng thời ra lệnh phát triển vũ khí và hệ thống phòng thủ dựa trên trí tuệ nhân tạo, dùng dữ liệu chiến trường đã tích lũy đến thời điểm đó. Với độc giả Hàn Quốc, đây là một cửa sổ hiếm hoi. Nhưng nguồn gốc của thông tin là chính phủ Ukraine và truyền thông địa phương. Đó là một bài viết truyền lại một tuyên bố của Ukraine qua một tầng trung gian, nghĩa là khoảng cách giữa phương hướng được công bố và kết quả thực sự được thực hiện chỉ có thể thu hẹp bằng cách đặt sổ sách mua sắm cạnh các kết quả trên chiến trường.

Có vài mục được cố ý để trống. Các nguồn thứ cấp lặp lại những câu nói rằng trong nhiều cuộc phỏng vấn sau khi nhậm chức, Fedorov đã viện dẫn kết quả kiểm toán nội bộ và đưa ra các con số về thâm hụt ngân sách của bộ, số nam giới không trình diện nhập ngũ, và số binh sĩ vắng mặt không phép. Một con số gây chú ý, được nói là mục tiêu về thương vong của phía Nga, cũng được trích dẫn cùng với các số liệu đó. Những con số ấy được giữ ngoài văn bản này.

Có hai lý do. Một là không thể đối chiếu nguyên văn và ngày tháng của những phát biểu đó với tài liệu gốc. Các con số được truyền qua những bản tóm tắt video rất dễ đổi đơn vị và mốc so sánh khi đi từ nơi này sang nơi khác. Lý do còn lại là ngay cả khi các phát biểu ấy là thật, đó vẫn là đánh giá của một bộ trưởng mới về quá khứ của chính bộ mình, và vị thế của nó khác với các số liệu được một cơ quan kiểm toán độc lập xác nhận. Khi thất bại của người tiền nhiệm được tô vẽ càng lớn, cải cách của người kế nhiệm càng hiện ra lớn hơn, và phát biểu mở đầu của một bộ trưởng mới được sinh ra bên trong cấu trúc ấy. Đây chính là nơi nguyên tắc không đặt

tuyên bố của chính phủ ngang hàng với kiểm chứng độc lập phải được áp dụng, và cho đến khi nền tảng đủ chắc, tốt hơn là để khoảng trống ấy nguyên vẹn.

Nếu chỉ viết trong phạm vi đã được xác nhận, thứ ông tiếp nhận là như sau: một bộ đang xử lý phần lớn ngân sách quốc gia trong lúc đánh mất niềm tin vì các vấn đề mua sắm; một lực lượng không người lái đã được thể chế hóa thành một quân chủng độc lập và đang vận hành; một tổ chức bị tổng thống công khai nêu tên để thay đổi hình thức; và một cuộc chiến khi ấy đã kéo dài gần bốn năm kể từ cuộc xâm lược toàn diện vào tháng 2 năm 2022. Trước mặt ông không phải là một trang giấy trắng, mà là một bản thảo đã được viết dở một nửa, và một phần trong bản thảo ấy chính ông đã viết từ bên ngoài.

Sức nặng của việc nói rằng Lực lượng Hệ thống Không người lái đã trở thành một quân chủng độc lập phải được đo bằng nghĩa thể chế. Theo một báo cáo nghiên cứu, lực lượng này có vị thế ngang với Lực lượng Tác chiến Đặc biệt và Lực lượng Phòng vệ Lãnh thổ. Tư lệnh đầu tiên của lực lượng, Vadym Sukharevskyi, đồng thời giữ chức cấp phó của Tổng tư lệnh Oleksandr Syrskyi. Việc lập một quân chủng, đặt một tư lệnh vào vị trí, và đưa lực lượng ấy vào chuỗi chỉ huy là thẩm quyền thuộc về lãnh đạo quân đội và tổng thống. Một bộ trưởng chuyển đổi số không có những thẩm quyền đó.

Về quy mô của bộ này cũng vậy, điều đã được xác nhận và điều nằm ngoài hồ sơ công khai tách ra khỏi nhau. Các khách mời trong podcast cuối tháng 1 nói rằng Bộ Quốc phòng xử lý một nửa ngân sách nhà nước của Ukraine. Đó là con số không thể đối chiếu với tài liệu ngân sách, nên nó đã được để ngoài phần chính của bản văn hiện tại. Tuy vậy, cả bài phát biểu của tổng thống lẫn phân tích bên ngoài đều chỉ về ít nhất một hướng: đây là bộ nơi tiền của quốc gia tập trung với khối lượng lớn.

Chính sách thay thế drone do Trung Quốc sản xuất bằng drone Ukraine cũng cần được tháo ra xem kỹ. Rất nhiều khung máy bay không người lái được dùng rộng rãi ngoài tiền tuyến ban đầu là drone thương mại do các công ty Trung Quốc bán cho người chơi sở thích và chụp ảnh. Chúng rẻ và dễ mua, nhưng đi kèm là nỗi lo rằng các công ty làm ra linh kiện và phần mềm có thể nhìn vào vị trí của khung máy bay hoặc tín hiệu điều khiển của nó. Còn có vấn đề nữa: nếu nguồn cung linh kiện bị cắt, toàn bộ lực lượng sẽ chao đảo. Tuyên bố của bộ trưởng mới rằng ông sẽ chuyển sang khung máy bay Ukraine là câu trả lời cho nỗi lo đó. Nhưng chính sách này đến với chúng ta dưới dạng bản tin thuật lại một thông báo của Ukraine, và việc thay thế thật sự đã diễn ra đến mức nào vẫn phải được xác nhận trong sổ sách mua sắm.

3. Thành công của Bộ Chuyển đổi Số có thể tồn tại khi không còn người sáng lập không?

Ngày 29 August 2019, ở tuổi hai mươi tám, Fedorov trở thành Bộ trưởng Chuyển đổi Số. Ông giữ chức vụ này hơn sáu năm bốn tháng, cho đến khi chuyển sang Bộ Quốc phòng vào January

2026, trở thành một trong những thành viên phục vụ lâu nhất trong nội các Ukraine. Trong thời gian đó, ứng dụng Diia do bộ của ông xây dựng đã trở thành một dịch vụ nhà nước được hơn 23 triệu người Ukraine sử dụng.

Liệu các chương trình hiện có có được vận hành theo cùng cách kể từ khi ông rời Bộ Chuyển đổi Số hay không, ở đây hồ sơ công khai cũng dừng lại. Các mạch vận hành của Diia, Brave1, và hệ thống mua sắm drone là những thiết chế, hay chúng là một con người cùng đội ngũ mà ông mang theo?

Một chương trình của chính phủ chỉ có thể được xem là đã trở thành một thiết chế khi nó tiếp tục vận hành sau khi người phụ trách thay đổi. Thành công bên trong chính phủ thường được tạo ra theo một trong hai cách. Một cách được khắc vào luật, ngân sách và sơ đồ tổ chức, để nó vẫn tiếp tục quay khi người giữ chức vụ thay đổi. Cách còn lại được một nhóm nhỏ có quyền đi vòng qua các quy tắc thúc đẩy với tốc độ cao. Trong vài năm đầu, nhìn từ bên ngoài, hai cách này khó phân biệt. Ứng dụng được tung ra, hợp đồng được ký, các chỉ số tăng lên. Khác biệt luôn hiện ra về sau, sau khi những con người ấy đã rời đi.

Như đã thấy, một phần đáng kể lý do khiến nền hành chính số của Ukraine vận hành nhanh nằm ở cách thứ hai. Quyết định nhanh, chuỗi phê duyệt được rút ngắn, khoảng cách gần với Office of the President. Đó là sức mạnh đã cứu dữ liệu của nhà nước trong năm đầu của cuộc chiến và viết lại các quy tắc mua sắm drone chỉ trong vài tháng. Khi một người sáng lập rời khỏi một tổ chức như vậy, thứ còn lại hoặc là một thiết chế đã được tôi cứng thành quy định, hoặc là cái vỏ rỗng của một vai trò mà con người gắn với nó đã biến mất.

Hồ sơ công khai hiện nay không đưa ra câu trả lời. Trong các tài liệu công khai đã được tham khảo, không có nguồn sơ cấp nào xác nhận ai kế nhiệm Fedorov làm Minister of Digital Transformation, hoặc người đó điều hành bộ như thế nào. Không có số liệu độc lập cho thấy các con số sử dụng Diia đã thay đổi ra sao sau khi ông rời đi. Không có tài liệu kiểm toán bên ngoài xác minh liệu các đánh giá và hợp đồng của Brave1 có còn quay với cùng tốc độ khi không có ông hay không. Lấp khoảng trống không có căn cứ bằng phỏng đoán, ta sẽ có những câu nghe hợp lý; chính những câu như vậy làm tiểu sử sụp xuống. Vì vậy, ở đây chỉ đặt ra hình dạng của câu hỏi, một cách chính xác. Câu trả lời thuộc về người khác, làm việc từ những nguồn khác, sau mốc khóa tư liệu ngày 13 July 2026.

Việc chính bản thân người đàn ông ấy đã chuyển sang nơi khác tự nó là một manh mối. Những việc Fedorov nói ông sẽ làm tại Ministry of Defence nằm trên cùng một đường với công việc ông đã làm tại Ministry of Digital Transformation. Đo kết quả bằng dữ liệu, đối xử với mua sắm như một chợ trực tuyến, nối các startup trực tiếp với quân đội. Điều ông nêu trong nghị trường như thành tích của mình cũng là số lượng công ty tư nhân đang chế tạo tên lửa và robot. Nếu phương pháp ấy đi từ bộ này sang bộ khác theo chân con người ấy, đó cũng là bằng chứng cho thấy phương pháp gắn với con người hơn là với tổ chức. Ngược lại, nếu Ministry of

Digital Transformation vẫn tiếp tục vận hành khi không có ông, thì sáu năm của ông là sáu năm ông đã thành công trong việc khiến chính mình có thể được thay thế. Cả hai khả năng vẫn còn mở, và nếu lúc này nghiêng ngòi bút về phía này hay phía kia, đó sẽ là chuyện thị hiếu chứ không phải bằng chứng.

Lịch chính trị cũng chồng lên câu hỏi này. Podcast phân tích vào cuối tháng 1 năm 2026 đã mô tả vốn chính trị của Fedorov như sau: tên ông chưa từng xuất hiện trong một vụ bê bối tham nhũng, ông không vướng vào các nhà tài phiệt mới, và niềm tin của công chúng dành cho ông ở mức cao. Cùng nhóm bình luận viên ấy đã nêu Fedorov và Budanov như những người kế nhiệm tiềm năng có thể nhắm tới thời kỳ hậu Zelensky, và cho rằng việc đưa một nhân vật như vậy vào một bộ dễ dính tham nhũng như Bộ Quốc phòng là một canh bạc rủi ro từ góc nhìn của tổng thống. Một bài viết tiếng Anh xuất bản vào mùa xuân năm 2026 cũng giới thiệu ông như một bộ trưởng quốc phòng được đánh giá cao. Nhưng cơ quan đó có tính chất gần với một nền tảng xúc tiến đầu tư và tuyên truyền đối ngoại cho Ukraine hơn. Những câu chữ thuận lợi không nên được đọc như một đánh giá độc lập.

Những nhận định này là phân tích chính trị và cảm nhận, không thể đặt ngang hàng với sự kiện đã được kiểm chứng. Nhưng cấu trúc mà phần phân tích chỉ ra vẫn đáng lưu ý. Một người đã biến danh tiếng trong sạch thành vốn chính trị nay nắm quyền tại bộ mà ở Ukraine, tiền bạc và nghi ngờ thường tụ lại cùng nhau. Liệu danh tiếng ấy có chịu nổi các sổ sách mua sắm của Bộ Quốc phòng và sống sót, hay sẽ bị thiêu rụi ở đó, thì với chứng cứ hiện có tính đến ngày 13 tháng 7 năm 2026, vẫn còn quá sớm để phán đoán. Viết rằng chưa thể đưa ra phán đoán cũng là một phần công việc của tiểu sử.

Nhìn vào các sự kiện đã được xác nhận: vào thời điểm ông đổi vai trò, hai quyền lực, dự án nhà nước số của Ukraine và quốc phòng quốc gia, đã gặp nhau trên lý lịch của một người. Người đã xây dựng Diia, người đã nối các mạch của mua sắm drone, người đã khởi động Brave1, nay là bộ trưởng của bộ mua tất cả những thứ đó. Có những quy tắc ông từng tạo ra từ bên ngoài, có những công ty đã lớn lên nhờ các quy tắc ấy, và giờ ông đứng ở phía ký hợp đồng với chính các công ty đó. Điều đó cũng có nghĩa là ông đã đến gần nơi một nhà cải cách chấm điểm kết quả cải cách của chính mình. Nên nhìn đây là cải cách đã hoàn tất hay là quyền lực bị tập trung vẫn là điều gây tranh luận ngay trong Ukraine, và để thuật lại cuộc tranh luận ấy một cách trung thực, trước hết phải xác định ai là người chỉ trích, rồi mới đến nội dung của lời chỉ trích.

Nghị quyết 4756-IX ngày 14 tháng 1 năm 2026 là một văn bản ngắn. Đằng sau văn bản ngắn ấy là sáu năm rưỡi của một con người, bắt đầu bằng một ứng dụng điện thoại thông minh, đi qua internet vệ tinh, gọi vốn cộng đồng và các nhà máy drone, rồi đến tòa nhà Bộ Quốc phòng. Tuy nhiên, liệu ông có giữ được cùng tốc độ ấy trong bộ hay không, thì ở đây hồ sơ công khai cũng dừng lại. Việc công nghệ đã khiến chính phủ nhanh hơn là điều đã được xác nhận. Liệu tốc

độ ấy có thể được duy trì bên trong một tổ chức nặng nề như quốc phòng quốc gia hay không, và nếu có thì với cái giá nào, chỉ có thể trả lời khi có thêm chứng cứ tích lũy.

Phép thử xem một thứ có sống sót như một thiết chế hay không không có gì quá bí ẩn. Đó là xem nó đã được khắc vào luật, ngân sách và sơ đồ tổ chức hay chưa. Nếu các tiêu chí đánh giá và thủ tục ký hợp đồng của Brave1 đã cứng lại thành quy định, cùng một tốc độ phải xuất hiện bất kể bộ trưởng là ai. Nếu chúng chỉ gắn với một con người, chuỗi phê duyệt sẽ lại dài ra. Những tài liệu cần để đưa ra phán đoán đó là hồ sơ vận hành của vị bộ trưởng kế nhiệm, thống kê sử dụng Diia, và kết quả kiểm toán bên ngoài đối với các hợp đồng của Brave1, nhưng cả ba đều không nằm trong phạm vi tài liệu đã thu được.

Vai trò mà ông đã bước sang cũng là nơi các lợi ích va chạm. Người từng làm ra luật chơi từ bên ngoài nay đứng về phía ký hợp đồng với các công ty đã lớn lên dưới chính các luật chơi ấy. Thứ kiểm soát một cấu trúc như vậy không phải là lương tâm của bộ trưởng, mà là các cơ quan kiểm toán và cơ quan chống tham nhũng. Và trong podcast cuối tháng 1 đã xuất hiện một cáo buộc rằng có những nỗ lực nhằm làm suy yếu chính các cơ quan chống tham nhũng đó. Không thể xác nhận cáo buộc ấy có đúng hay không. Nếu đúng, vấn đề một người tự chấm điểm cuộc cải cách của mình còn lớn hơn nữa.

Những đánh giá về ông có trọng lượng khác nhau tùy theo xuất xứ. Câu nói rằng ông trong sạch và được tin cậy cao đến từ các khách mời trong một podcast chính sách. Mô tả ông là một bộ trưởng quốc phòng được đánh giá cao nằm trong một bài viết gửi đăng ở một ấn phẩm gần với quảng bá đầu tư và tuyên truyền đối ngoại cho Ukraine hơn. Bản tin tiếng Hàn về đường hướng của ông ngay sau khi nhậm chức thuật lại một thông báo của chính phủ Ukraine qua một lớp trung gian. Cả ba đều đáng đọc, và không cái nào trong ba cái là một cuộc kiểm toán độc lập. Câu trả lời cho việc sáu năm rưỡi của ông là một thiết chế hay chỉ là một con người sẽ không đến từ ba loại bài viết này, mà từ sổ sách của Bộ Chuyển đổi Số khi không còn ông và Bộ Quốc phòng khi có ông.

Chương 10. Một quân đội được chỉ huy bằng dữ liệu và AI

1. Vong mach cua diem tan cong, don dat thiet bi va du lieu mua sam

Ngay 26 January 2026, Bo Quoc phong Ukraine thong bao rang trong nam 2025, cac luc luong cua nuoc nay da tan cong khoang 820,000 muc tieu cua Nga. Con so nay do Bo truong Mykhailo Fedorov dua ra va la thong ke rieng cua bo, duoc tinh dua tren mot he thong diem do chinh bo van hanh.

De hieu con so do, truoc het phai nhin vao cach no duoc dem. He thong nay co ten Army of Drones Bonus, va o Ukraine nguoi ta thuong goi la e-points. Khi mot don vi danh trung thiet bi cua doi phuong hoac mot vi tri phong thu kien co, drone ghi hinh khoanh khac do, roi don vi tai doan phim len lam bang chung. Nhung ket qua duoc xac nhan bang video se duoc gan diem, va diem tich luy trong tai khoan cua don vi. Don vi sau do mang so diem nay vao mot cho truc tuyen do nha nuoc van hanh, chon drone va thiet bi ma ho thuc su muon dung, con nha nuoc tra tien cho nha san xuat.

Ho so cua mot nguoi linh ve viec tieu diet doi phuong duoc chuyen thanh suc mua doi voi vu khi ma nguoi linh do se cam tiep theo. Trong mot quan doi noi nhung nguoi mua vu khi va nhung nguoi dung vu khi tu lau da gan nhu khong bao gio gap nhau, he thong nay la mot no luc ep hai nhom do lai gan nhau. Phuong phap ma Fedorov lap lai trong nhung nam lam bo truong chuyen doi so lai hien len: bien hanh vi thanh du lieu, roi bien du lieu do thanh tieu chi de phan bo tien va materiel.

Khi các điểm số trở thành mệnh lệnh, mệnh lệnh để lại dấu vết mua sắm. Theo một thông báo của bộ vào ngày 11 March 2026, các lữ đoàn chiến đấu đã nhận 500,000 hạng mục, trong đó có drone và hệ thống robot mặt đất, thông qua DOT-Chain Defence, kênh mua sắm số do cơ quan mua sắm hậu cần vận hành. Con số này cũng là thống kê của chính bộ. Hệ thống robot mặt đất là các phương tiện không người lái di chuyển trên mặt đất bằng bánh xe hoặc xích, dùng để kéo người bị thương ra ngoài hoặc chở đạn dược. Cùng ngày, bộ thông báo rằng họ đã ký hợp đồng mua drone multirotor với quy mô kỷ lục. Multirotor là loại máy bay bay bằng nhiều cánh quạt; chiếc drone bốn cánh quen thuộc trong các bức ảnh thuộc nhóm này.

Việc hai thông báo được đưa ra cùng một ngày không giống một sự trùng hợp. Một thông báo nói về những gì tiền tuyến đã nhận và số lượng bao nhiêu. Thông báo kia nói về những gì nhà nước mới mua và mua bao nhiêu. Con số thứ nhất nâng đỡ con số thứ hai. Thứ mà một đơn vị chọn trở thành tín hiệu nhu cầu, và tín hiệu ấy trở thành cơ sở cho hợp đồng tiếp theo. Đó là nguyên tắc thị trường, rằng hàng hóa bán chạy sẽ được sản xuất nhiều hơn, được đưa vào thủ tục mua sắm của quân đội; thứ mà bộ của Fedorov gọi là vòng tuần hoàn dữ liệu là một cặp mũi tên chỉ về hai hướng ngược nhau: dữ liệu hiệu suất đi từ tiền tuyến về hậu phương, vật tư đi từ

hậu phương ra tiền tuyến.

Mission Control là nỗ lực đưa thêm trục thời gian và con người vào vòng tuần hoàn này. Ngày 23 January 2026, Fedorov ký lệnh khởi động hệ thống chỉ huy và kiểm soát drone này trong hệ sinh thái số chiến đấu DELTA, tuyên bố rằng mọi hoạt động drone sẽ được gắn vào một hệ thống số duy nhất. Phạm vi mà bộ trưởng mô tả trong thông báo của bộ rất rộng. Nhiệm vụ nào đã được thực hiện với cường độ ra sao, từng tổ vận hành đã làm gì, một cá nhân cụ thể ở lại tuyến đầu trong bao lâu, bao nhiêu hoạt động hậu cần được thực hiện thay cho cá nhân đó, tất cả đều được đọc như dữ liệu.

Mô tả này là lời trình bày của chính bộ trưởng và là kế hoạch được nêu vào thời điểm khởi động. Trong hồ sơ công khai không có tài liệu nào cho thấy một nhà nghiên cứu hoặc cơ quan kiểm toán bên ngoài bộ đã xem xét và xác nhận Mission Control thực sự xử lý những gì. Một tuyên bố về điều người ta định làm và một báo cáo về điều người ta đang làm nằm ở hai tầng khác nhau, nhưng trong các thông báo của chính phủ, hai thứ ấy thường xuất hiện trong cùng một câu, khiến người đọc phải tự tách chúng ra.

Nguồn gốc của DELTA nằm ở một công cụ nhận thức tình huống do Aerorozvidka, một tổ chức tình nguyện dân sự, xây dựng sau năm 2014. Gọi DELTA là sản phẩm do Fedorov tạo ra là rời khỏi sự thật. Hệ thống này đã ổn định với tư cách một hệ thống nhà nước từ rất lâu trước khi ông trở thành bộ trưởng quốc phòng, và chữ ký vào tháng 1 năm 2026 chỉ là việc bổ sung một module vào một hệ thống vốn đã vận hành. Bỏ lỡ sự phân biệt này, mười hai năm lao động tích lũy của một quốc gia sẽ bị đọc thành thành tựu của một người.

Mạch vận hành càng lớn, mắt người càng tụt lại phía sau. Một báo cáo phân tích ghi nhận rằng từ năm 2024 đến năm 2025, DELTA đã xử lý dữ liệu tình báo, giám sát và trinh sát (ISR) lên tới hàng chục terabyte mỗi ngày. Tình báo, giám sát và trinh sát là thuật ngữ quân sự bao trùm toàn bộ hoạt động tìm hiểu kẻ địch đã đặt gì ở đâu, và đang làm gì tại đó; hình ảnh từ drone, quan sát pháo binh, và báo cáo trinh sát đều nằm trong phạm vi này. Một terabyte có thể chứa vài trăm bộ phim độ nét cao, và khối lượng ấy chồng lên từng ngày.

Vì vậy, vấn đề của người chỉ huy đã chuyển từ nhìn thấy nhiều hơn sang chọn nhanh hơn. Nếu mắt người không thể xem hết hàng chục terabyte, việc lọc sẽ rơi vào máy móc. Phần mềm đảm nhận công việc thu hẹp các mục tiêu ứng viên, xóa những bản trùng của cùng một cảnh, và xếp hạng mục tiêu nào nên bị tấn công trước. DELTA, chạy trên nền tảng đám mây, gửi bức tranh đã được lọc này xuống cả bộ chỉ huy cấp cao lẫn các đơn vị cấp dưới. Một báo cáo nhận xét rằng thiết kế này trao cho cả các đơn vị tiền tuyến và sĩ quan cấp thấp năng lực nhận thức tình huống của một chỉ huy cấp cao. Đó là một cấu trúc nhằm để chiến trường tự phán đoán, không phải đi qua nhiều mắt xích trong chuỗi báo cáo.

Phán đoán càng nhanh, khoảng trống để nền tảng của phán đoán ấy trôi qua mà không có con người kiểm chứng càng lớn. Những quy tắc nào đã tạo ra một màn hình nhất định, ai kiểm

toán thuật toán đó, trách nhiệm nằm ở đâu khi đánh giá mục tiêu sai, không điều nào trong số này xuất hiện trong các thông báo của bộ. Điều tương tự cũng xảy ra vào ngày 9 tháng 4 năm 2026, khi bộ ra thông cáo giới thiệu Drone Line như sự thực thi một học thuyết chiến tranh mới. Cách diễn đạt đầy tham vọng, nhưng đến nay vẫn chưa có đánh giá độc lập nào về việc Drone Line thật sự tạo ra gì ở mặt trận. Khoảnh khắc một thông báo của chính phủ được xử lý với cùng trọng lượng như một sự kiện đã được kiểm chứng, tiểu sử trượt sang bản sao quảng bá.

DELTA mất nhiều năm mới trở thành một hệ thống cấp nhà nước. Từ năm 2017, nó được thử nghiệm như một công cụ phối hợp quân sự, nhưng lúc đầu nền tảng thể chế còn mỏng; nhờ sự hỗ trợ từ một quỹ tín thác của NATO, khoảng năm 2019 nó bắt đầu đạt được các chứng nhận về khả năng tương tác. Khả năng tương tác có nghĩa là thiết bị và định dạng tài liệu của quân đội nhiều quốc gia khác nhau có thể ăn khớp và vận hành cùng nhau. Khi được bộ chính thức phê duyệt vào năm 2023, DELTA đổi tính chất: từ một chương trình hiển thị bản đồ thành một định dạng tích hợp, nối nhiều hệ thống thành một khối.

DELTA không hẳn là một chương trình riêng lẻ, mà giống một chiếc ô bao trùm nhiều mô-đun. Bên dưới nó có Monitor, công cụ theo chuẩn bức tranh tác chiến chung của NATO; Vezha, công cụ truyền trực tiếp hình ảnh từ drone theo thời gian thực; Element, công cụ chuyển tin nhắn mã hóa; và Target Hub, công cụ quản lý lịch sử của một mục tiêu từ khi phát hiện đến khi xử lý xong. Bức tranh tác chiến chung là sự thống nhất cho phép nhiều đơn vị nhìn cùng một bản đồ với cùng một hệ thống ký hiệu. Mission Control, do Fedorov ra mắt vào tháng 1 năm 2026, là một khoang mới được treo dưới chiếc ô này; ông không phải là người dựng lên chính chiếc ô đó.

Cuộc kiểm toán an ninh thông tin năm 2024 của DELTA đã được trình bày ở Chương 8. Cuộc kiểm toán đó xử lý vấn đề bảo mật của hệ thống và chứng nhận theo tiêu chuẩn NATO; nó không xác minh các con số tấn công mà DELTA ghi nhận.

2. Phòng không, drone đánh chặn, sĩ quan số và đánh giá sau hành động

Cuộc chiến trên bầu trời đêm Ukraine năm 2026 là cuộc chiến hỏa lực, và cũng là cuộc chiến của phép tính. Một báo cáo phân tích ghi nhận rằng khoảng cách chi phí giữa bên tấn công và bên phòng thủ đã mở ra ở mức xấp xỉ 26 trên 1. Để bắn hạ một máy bay không người lái tự sát giá rẻ, bên phòng thủ phải tiêu hao một khí tài đắt hơn khoảng hai mươi sáu lần. Bỏ mặc nó thì nhà máy điện và khu chung cư bị phá hủy; cố chặn nó thì tên lửa phòng không quý giá biến mất. Báo cáo gọi thế lưỡng nan này là chi phí của việc không hành động. Trong một tình thế mà lựa chọn nào cũng phải trả giá, quốc gia phòng thủ nghèo đi thêm một chút ngay cả khi giành phần thắng.

Cách tính của Russia đi theo hướng nới rộng khoảng cách đó. Theo cùng báo cáo, Russia đã ký với Iran một hợp đồng sản xuất trị giá 1.75 billion dollars tại đặc khu kinh tế Alabuga ở

Tatarstan, thỏa thuận chế tạo khoảng 6,000 máy bay không người lái vào năm 2025. Thân máy bay cũng thay đổi. Dòng gọi là Black Shahed được đưa ra chiến trường, phủ vật liệu hấp thụ radar và sơn đen để radar và mắt người khó bắt được hơn, đồng thời gắn ăng-ten thích ứng có thể lọc nhiễu gây nhiễu điện tử. Để bào mòn phòng không Ukraine mà không đem lại mục tiêu thật, một máy bay không người lái mồi nhử giá rẻ tên Gerbera xuất hiện, làm bằng expanded polystyrene, tức styrofoam. Đơn giá mà báo cáo nêu cho Gerbera vào khoảng 1,000 dollars mỗi chiếc. Khi việc phóng một tên lửa trị giá hàng trăm nghìn dollars vào một mục tiêu giả trị giá 1,000 cứ lặp lại đêm này qua đêm khác, bên phòng thủ sụp xuống trong khi vẫn khoe tỷ lệ đánh chặn. Đó là hình dạng của bài toán mà phòng không Ukraine phải giải.

Ukraine xây dựng một hệ thống kết nối các đơn vị ngoài chiến trường, cơ quan mua sắm và bộ quốc phòng. Thiết kế dự phòng, tức đặt mọi thứ thành nhiều lớp để khi một lớp nhường chỗ thì lớp khác giữ lại, cũng lặp lại trên bầu trời.

Lớp dưới cùng là sự hồi sinh của vũ khí cũ. Pháo phòng không tự hành Gepard do Germany chuyển giao đã trở thành một trụ cột trong đánh chặn máy bay không người lái. Pháo phòng không tự hành là khung thân xe tăng gắn pháo phía trên, chĩa lên bầu trời, và đạn pháo của nó rẻ hơn tên lửa rất nhiều. Các thiết bị phòng không tầm ngắn thời Soviet, ZU-23-2, ZSU-23-4 Shilka, 2S6 Tunguska, lại quay nòng lên trời. Đầu năm 2022, một hệ thống phòng không Pantsir-S1 của Russia bị thu giữ đã được sửa chữa, đưa vào hoạt động và được ghi nhận bắn hạ mục tiêu. Dù người ta nói nhiều về một cuộc chiến công nghệ cao, thứ chống đỡ tầng nền của phòng không lại là pháo tự động cũ.

Phía trên lớp đó là một tấm lưới biết lắng nghe. Ukraine đã mắc hàng nghìn cảm biến âm thanh thụ động lên các tháp thông tin liên lạc và cột điện trong một mạng lưới có tên Zvook. Cảm biến thụ động không tự phát ra tín hiệu nào; nó chỉ ghi nhận âm thanh. Một thuật toán được huấn luyện trên dấu hiệu âm thanh của động cơ drone Shahed sẽ nhận ra thân bay chỉ từ âm thanh ấy. Vì nó không phát sóng vô tuyến như radar, vị trí của chính cảm biến không bao giờ bị lộ. Các phát hiện thu được theo cách này được đưa vào những hệ thống chỉ huy như Virazh và Safe Sky, rồi mục tiêu được giao cho các đội hỏa lực cơ động trang bị đèn rọi và súng máy hạng nặng. Năm 2024, thiết bị quan sát có camera ảnh nhiệt được bổ sung, cho phép xác định chính xác tầm xa và độ cao. Một radar của Hà Lan triển khai tại Ukraine phân biệt chim với drone bằng quy trình xử lý đọc các thành phần rung động cực nhỏ. Đó là cách rải rộng các cảm biến rẻ tiền và nối tín hiệu của chúng lại bằng phần mềm; điều Zvook làm với dữ liệu âm thanh chính là điều DELTA đã làm với dữ liệu mục tiêu.

Lớp trên cùng là drone đánh chặn. Thay vì dùng tên lửa, một drone bắt một drone khác. Dòng drone đánh chặn STING được nêu trong báo cáo có giá khoảng 2.500 đô la mỗi chiếc và mang một mô-đun tự truy đuổi, tự ngắm vào Shahed. Nếu một thân bay 2.500 đô la nhận phần việc của một quả tên lửa có giá hàng trăm nghìn đô la, dấu trước khoảng chênh chi phí 26 trên

1 ấy sẽ đảo chiều. Báo cáo viết rằng thay đổi này đang viết lại luật chơi của không chiến.

Báo cáo đó cũng chỉ ra nơi tấm lưới bị rách: bom lượn có điều khiển của Nga, KAB và FAB. Đây là những quả bom cũ được gắn cánh và bộ dẫn đường, rồi được thả từ xa. Chúng khó bị gây nhiễu, khó bị đánh chặn, và có thể đánh sập nguyên vẹn các vị trí cùng công trình gần tiền tuyến. Báo cáo cho rằng cần tăng sản lượng các tên lửa châu Âu nhỏ hơn, rẻ hơn, có khả năng bắn hạ drone cấp Shahed, đồng thời nên tính đến phương án đưa các cơ sở công nghiệp quốc phòng châu Âu xuống dưới lòng đất trong kịch bản xấu nhất. Bầu trời nơi kinh tế học của drone đánh chặn vận hành rất đẹp và bầu trời nơi vẫn chưa có lời giải thực ra là cùng một bầu trời; vì vậy, nếu chỉ nói về thành công của phòng không thì mới kể được nửa câu chuyện.

Trong kho lưu trữ công khai không có hồ sơ nào cho thấy quân đội Ukraine mới lập một chức danh gọi là "sĩ quan kỹ thuật số". Cũng không có tài liệu gốc nào trình bày việc after-action review, tức quy trình một đơn vị tập hợp sau chiến dịch để truy ngược lại những gì đã sai, đã thay đổi ra sao trong quân đội Ukraine. Vì thế, chức danh ấy và cuộc họp ấy đã được để ngoài văn bản này. Những gì tài liệu thật sự cho thấy chỉ là bằng chứng gián tiếp rằng vai trò này đang dịch chuyển từ con người sang phần mềm, và mức xác nhận chỉ đến đó.

Một tạp chí quân sự đã bàn về cách công việc của người điều phối tấn công đầu cuối chung (JTAC) đang thay đổi. JTAC là sĩ quan tiến lên phía trước và dẫn máy bay của lực lượng mình vào các đòn đánh. Trước đây, công việc này nghĩa là đọc tọa độ bằng giọng nói qua radio và kiểm soát trình tự ném bom; nay các máy bay không người lái nhỏ và thiết bị chỉ thị mục tiêu bằng laser đảm nhận vai trò đó. Tạp chí ấy đẩy ý tưởng đi thêm một bước, tới thứ mà họ gọi là Artificial RTO, tức điện thoại viên vô tuyến nhân tạo. Hình dung ở đây là phần mềm trí tuệ nhân tạo nằm bên trong hệ thống thông tin liên lạc, xử lý lưu lượng thoại, thông tin địa lý và tài liệu học thuyết theo thời gian thực, rồi tiếp quản việc tính toán mục tiêu, chỉ để con người giữ quyền phê chuẩn cuối cùng.

Hình dung này là một đề xuất được đăng trên tạp chí, không phải một hệ thống mà quân đội Ukraine đã vận hành, và sự phân biệt đó sẽ không bị làm mờ ở đây. Nhưng hướng đi của đề xuất ấy cũng là hướng mà DELTA và Mission Control đang tiến tới. Đó là một thiết kế giao việc sắp xếp và tính toán, vốn từng do con người làm, cho máy móc, rồi chỉ để con người đưa ra quyết định cuối cùng. Quyết định cuối cùng ấy có thật sự là phán đoán của con người hay chỉ là thủ tục đóng dấu lên một danh sách mà máy đã thu hẹp sẵn, bản thiết kế tự nó không trả lời được câu hỏi này.

Với việc rút kinh nghiệm sau hành động, tình hình hơi khác. Một báo cáo về DELTA nêu riêng vòng phản hồi nhanh từ người vận hành tới nhà phát triển như một tính năng của hệ thống. Một vấn đề mà người lính ở tiền tuyến gặp phải sẽ nhanh chóng tới tay nhà phát triển, và phần mềm đã sửa được đưa trở lại tiền tuyến. Đặt Mission Control lên trên đó, nhiệm vụ nào thành công và tổ bay nào đã làm gì vẫn được giữ lại như dữ liệu trong khi chiến dịch diễn ra hoặc ngay

sau đó.

Các báo cáo được lưu giữ dưới dạng hồ sơ máy tính, và những người chịu trách nhiệm theo dõi tiến độ trên bảng điều khiển. Có thể gọi đây là một cuộc rút kinh nghiệm sau hành động bằng kỹ thuật số. Nhưng ngay khi gọi như vậy, một điều gì đó đã trượt mất. Rút kinh nghiệm sau hành động theo cách truyền thống là nơi con người tranh luận thành tiếng về lý do họ thất bại. Nhật ký cho bạn biết chuyện gì đã xảy ra; nó không cho bạn biết vì sao người chỉ huy đã phán đoán như vậy vào đúng khoảnh khắc đó. Mạch phản hồi mà bộ của Fedorov đã xây dựng có thể thay thế câu hỏi đầu tiên hay âm thầm xóa mất câu hỏi thứ hai, đó không phải là điều các tài liệu hiện nay có thể trả lời.

Một điều vẫn rõ ràng. Khi Mission Control đề xuất đọc cả số giờ của từng người lính ở sát tiền tuyến và khối lượng hậu cần đã di chuyển vì người đó, hệ thống ấy trở thành công cụ theo dõi chính phía mình không kém gì công cụ theo dõi đối phương. Một bộ máy đo hiệu suất luôn đồng thời là một bộ máy đo con người, và hai chức năng ấy chạy chung trên cùng một nguồn dữ liệu.

Nguồn gốc của những thiết bị đang đỡ phần nền của phòng không còn làm tính chất của cuộc chiến này hiện ra rõ hơn. Gepard được thiết kế tại Tây Đức, do KNDS chế tạo bằng cách đặt một pháo phòng không lên thân xe tăng Leopard 1. Những mục tiêu mà Zvook bắt được bằng âm thanh được chuyển cho các tổ hỏa lực cơ động, được trang bị đèn rọi, súng máy hạng nặng DShK và súng Maxim lắp đôi. Maxim là súng máy từ Thế chiến thứ nhất, còn bộ ngắm Skylark gắn lên nó vào năm 2024 dùng camera nhiệt để xác định cự ly và độ cao. Một khẩu súng từ một thế kỷ trước và một bộ phân loại âm thanh AI đứng cùng một vị trí.

Sự tiến hóa của các khung máy bay Nga chỉ được mô tả đến mức báo cáo ghi lại. Dòng Black Shahed được lắp modem 4G/LTE và liên lạc Starlink, còn ăng-ten thích ứng lọc nhiễu gây chế áp được gọi là Kometa. Mồi nhử Gerbera không chỉ rẻ; nó được chế tạo để bắt chước tín hiệu phản xạ radar mà drone tấn công thật, Geran-2, để lại. Làm cho người quan sát không thể phân biệt giả và thật trên màn hình chính là mục đích của khung máy bay này. Xử lý micro-Doppler mà radar Hà Lan triển khai ở Ukraine dùng để đọc các rung động nhỏ do cánh quạt quay tạo ra, từ đó tách chim ra khỏi máy bay.

Ở đây cần thận trọng. Tỷ lệ chi phí 26 trên 1, con số 2.500 đô la cho STING, con số 1.000 đô la cho Gerbera, tất cả đều là những con số được ghi trong một báo cáo phân tích duy nhất. Chúng không phải giá mua sắm theo đơn vị do chính phủ Ukraine công bố, cũng không phải bảng giá chính thức của nhà sản xuất, và trong hồ sơ công khai không có thống kê độc lập nào cho biết drone đánh chặn thực sự hạ được bao nhiêu phần trăm Shahed. Khái niệm Artificial RTO cũng vậy: trong một thiết kế chỉ để con người giữ quyền phê chuẩn cuối cùng, con người ấy dựa vào đâu để phê chuẩn, và cần thủ tục nào để đảo ngược danh sách mà máy đã thu hẹp, tạp chí đó cũng không ghi lại.

3. Cải cách mua sắm và vấn đề xác minh kết quả trên chiến trường

Bộ Quốc phòng Ukraine từng hứng chịu chỉ trích nặng nề vì tham nhũng trong mua sắm thực phẩm và quân phục. Những hợp đồng mua khẩu phần ăn và quần áo cho quân đội với giá phi lý bị phanh phui, và toàn bộ hệ thống mua sắm bị đặt lên bàn mổ. Việc tiền tuyến thiếu đạn pháo trong khi giá trứng ở hậu phương bị đội lên được công chúng nhìn như một kiểu phản bội khó chấp nhận.

Sau đó, hai cơ quan mua sắm chuyên trách được thành lập. Defence Procurement Agency (DPA) phụ trách thiết bị sát thương như vũ khí và đạn dược; State Rear Operator (DOT) phụ trách vật tư không sát thương như thực phẩm và quần áo. Các hội đồng giám sát gồm chuyên gia trong nước và nước ngoài được gắn vào hệ thống, và hợp đồng được đăng trên các nền tảng mua sắm mở như ProZorro. ProZorro là cổng mua sắm công của Ukraine, được xây dựng để người dân có thể tra cứu qua internet ai đã mua thứ gì với giá bao nhiêu. Đến đây, mọi việc đi đúng trình tự cải cách như trong sách giáo khoa.

Trong hệ thống mới, các vấn đề cũ lại xuất hiện. Để ngăn hàng lỗi ra tiền tuyến, DPA lập nhiều tầng kiểm tra chất lượng và một hệ thống phạt theo hợp đồng. Rắc rối nằm ở thời gian. Nhiều tháng trôi qua trong lúc các thủ tục kiểm tra và tuân thủ tiêu chuẩn được xử lý, còn chu kỳ công nghệ của cuộc chiến drone lại ngắn hơn chừng ấy tháng. Khi một chiếc drone đã được xác minh hoàn hảo cuối cùng cũng tới tiền tuyến, có những trường hợp thiết bị tác chiến điện tử mới của Nga đã chặn mất tần số mà chiếc drone đó dùng. Tác chiến điện tử là cuộc đấu nhằm gây nhiễu hoặc chặn bắt tín hiệu vô tuyến, cắt đứt liên lạc và quyền điều khiển của đối phương. Đó là nghịch lý của một vũ khí được xác minh hoàn hảo trên giấy nhưng mất tác dụng ngoài thực địa. Xác minh càng chặt, vũ khí càng đến muộn; đến càng muộn, ý nghĩa của việc xác minh càng tan biến.

Sự thiếu hụt thiết bị và gánh nặng chi phí sửa chữa lại đổ lên vai binh sĩ. Một báo cáo đã phê phán cơ cấu này là kiểu mua sắm mang tính phản ứng. Bộ mua vũ khí với số lượng lớn để giữ cho dây chuyền sản xuất tiếp tục vận hành rồi xếp chúng trong kho, nhưng đến khi chúng tới tay người dùng cuối thì đã lỗi thời và phải gửi về tuyến sau để xử lý. Khi cạnh tranh về giá buộc nhà sản xuất cắt giảm chi phí, gánh nặng thử nghiệm, sửa lỗi và cải tiến chuyển sang các đơn vị tiền tuyến. Đã có những trường hợp được ghi nhận trong đó một phần đáng kể số drone được giao chỉ có thể bay sau khi đơn vị tháo chúng ra và làm lại, rồi tình trạng người điều khiển vừa là thợ máy vừa là nhà phát triển trở thành chuyện cố định.

Các con số liên quan cho thấy gánh nặng ngoài chiến trường nặng đến mức nào. Theo một báo cáo mua sắm, các phi công drone ở tiền tuyến đang phải tự bỏ tiền túi, từ 5 đến 30 phần trăm mức lương tháng khoảng 3,000 dollars, để chỉnh sửa và cải thiện thiết bị của mình. Trong khi nhà nước tuyên bố đã thực hiện thành công các gói mua sắm trị giá hàng tỷ, tiền lương của binh sĩ lại đang bù vào những thiếu sót của vũ khí. Thành công trên hồ sơ mua sắm và thành

công trên chiến trường đang được ghi vào hai cuốn sổ khác nhau.

Bên theo dõi dòng tiền cũng có những bức tường riêng. Một báo cáo về quản lý quỹ viện trợ quốc tế chỉ ra rằng trong mua sắm thời chiến, điều khó xử lý hơn cả tham ô trực tiếp là rủi ro ủy thác gián tiếp: thổi phồng đơn giá, đổi chất lượng lấy số lượng, gây sức ép để chứng nhận giao hàng thật nhanh. Ngay cả khi số lượng ghi trên giấy được chứng nhận là đã giao đủ chính xác, việc hàng hóa có đạt chất lượng mà chiến trường đòi hỏi hay không rất khó xác lập chỉ bằng kiểm soát sau đó. Vì vậy Ukraine và các quỹ liên kết với World Bank đã đưa vào quy trình chuẩn hóa và giám sát của bên thứ ba. Giám sát bên thứ ba là khi một tổ chức bên ngoài, không phải bên cấp tiền cũng không phải bên nhận tiền, đi xuống thực địa và đối chiếu hàng hóa với sổ sách. Ở sát tiền tuyến, nơi không ai có thể vào, không có cách nào tiến hành kiểm tra tại chỗ; vì thế nơi cần xác minh nhất lại vẫn là nơi khó xác minh nhất.

Câu trả lời từ phía Fedorov không đi theo hướng thêm nhiều cuộc kiểm toán. Nó đi theo hướng chuyển chính tiêu chuẩn xác minh, và hệ thống e-points đã nói ở trên chính là bước chuyển đó. Thay vì một công chức xem xét giấy tờ rồi phê duyệt, đoạn phim phá hủy mục tiêu do đơn vị quay trở thành bằng chứng về hiệu quả. Hiệu quả biến thành điểm, điểm biến thành sức mua, và các đơn vị chọn drone từ những nhà sản xuất mà họ đã tự thử và bắt đầu tin cậy. Lô-gic ở đây là hàng lỗi sẽ bị lọc ra vì chính người sử dụng là người lựa chọn. Báo cáo mua sắm ghi nhận rằng một cách tiếp cận DeCenter cũng đang được thử nghiệm, trao cho các lữ đoàn quyền mua trực tiếp drone và thiết bị tác chiến điện tử từ nhà sản xuất bằng ngân sách nhà nước. Đơn vị chi ngân sách tốt sẽ được phân bổ nhiều hơn vào tháng sau; tiền không dùng hết sẽ bị thu hồi. Tính bằng hryvnia, tiền tệ của Ukraine, một lữ đoàn Territorial Defense đã thực hiện 1 billion hryvnia, khoảng 25 million dollars, chỉ trong một năm, vượt xa mức 1 đến 1.5 million dollars của ngân sách lữ đoàn trung bình.

Kiến trúc của hệ thống có những ưu điểm rõ ràng. Đồng thời, thiết kế này không xóa bỏ vấn đề kiểm chứng, mà chủ yếu chuyển nó sang một vai trò khác.

Một vai trò mà vấn đề ấy được chuyển sang là bảng chấm điểm. Khi nhà nước quyết định một mục tiêu nhất định đáng giá bao nhiêu điểm, các đơn vị sẽ đuổi theo những mục tiêu có điểm cao, và bảng chấm điểm trở thành học thuyết chiến thuật. Chưa có tài liệu nào được thu thập cho thấy ai lập và sửa bảng này, theo thủ tục nào, hoặc quá trình đó có thể được nhìn thấy từ bên ngoài hay không.

Độ tin cậy của việc phán định qua video dẫn tới cùng một vấn đề. Xác định sự phá hủy dựa trên hình ảnh quay được từ lâu đã là điểm tranh cãi trong mọi cuộc chiến. Không tìm thấy tài liệu độc lập nào cho biết ai đưa ra kết luận này, phản đối được nêu ra ra sao, hoặc có bao nhiêu phán đoán sai. Con số 820.000 mục tiêu trong năm 2025 do chính bộ đưa ra là tổng số được xây trên thủ tục phán định này, nên nếu thủ tục chưa được kiểm chứng, tổng số ấy cũng chưa được kiểm chứng.

Xem tốc độ chi tiền là thành tích cũng có rủi ro riêng. Một quy tắc cấp nhiều tiền hơn cho các đơn vị tiêu tiền nhanh sẽ phá vỡ bộ máy hành chính chậm chạp. Nó cũng để ngỏ khả năng tiêu nhanh và tiêu tốt bị tính như cùng một việc. Một thước đo đo tốc độ thì chỉ đo tốc độ mà thôi.

Nhưng vẫn còn những câu hỏi mà kết quả chưa được công bố. Chưa có báo cáo kiểm toán bên ngoài nào xem xét toàn bộ vòng vận hành này được đưa ra. Không có tài liệu nào xác minh độc lập Army of Drones Bonus, DOT-Chain Defence, hay các kết quả mua sắm được xếp lên trên chúng. Con số 500.000 hạng mục và hợp đồng drone quy mô kỷ lục được công bố ngày 11 March 2026 là những số liệu do chính bộ này đưa ra, theo dạng tự báo cáo tại thời điểm công bố.

Một báo cáo chính sách đã tóm lại bài học của cuộc chiến này như sau: công nghệ không tự nó trở thành sức mạnh chiến đấu, và chỉ khi chính sách, mua sắm và học thuyết cùng chuyển động thì công nghệ mới biến thành sức mạnh quân sự. Bộ của Fedorov đã cố chuyển câu ấy thành thể chế. Bộ này xây một vòng vận hành trong đó một đòn tấn công biến thành điểm, điểm biến thành đơn hàng, đơn hàng biến thành dữ liệu hợp đồng, rồi dữ liệu hợp đồng lại biến thành vật tư và đi xuống tiền tuyến. Từ thủ tục mua một linh kiện riêng lẻ đến cách một lữ đoàn thực thi ngân sách, vòng vận hành này đã buộc tay chân quân đội vào dữ liệu.

Vòng vận hành ấy thực sự nhanh hơn bao nhiêu, và liệu nó có chính xác tương xứng với tốc độ hay không, vẫn chưa có câu trả lời. Những tài liệu có thể tạo ra câu trả lời vẫn chỉ nằm ở một phía. Tính đến 13 July 2026, sau sáu tháng Fedorov giữ chức bộ trưởng quốc phòng, nội dung thực chất của các tài liệu mô tả vòng vận hành này đến từ chính bộ đang vận hành nó. Đây không phải là lời cáo buộc, mà là mô tả một tình trạng. Ở một quốc gia đang có chiến tranh, kiểm toán bên ngoài chậm lại là chuyện thường gặp. Nhưng nếu sự chậm trễ kéo dài, tình trạng bên tuyên bố kết quả và bên xác nhận kết quả là cùng một người sẽ đông cứng lại, và một quân đội được chỉ huy bằng dữ liệu sẽ biến thành một quân đội được chỉ huy bởi những người tạo ra dữ liệu.

Hãy nhìn lại nội dung chính của cuộc cải cách. Mua sắm được đưa ra khỏi tay trụ sở bộ và chuyển sang các cơ quan riêng; các hội đồng giám sát gồm chuyên gia trong nước và nước ngoài được đặt phía trên những cơ quan ấy; hợp đồng được đăng trên ProZorro để người dân kiểm tra. Thiết kế này nhằm ngăn nạn tham nhũng kiểu trứng và áo khoác tái diễn, chứ không nhằm đưa vũ khí ra tiền tuyến nhanh hơn. Hai mục tiêu ấy gặm mòn nhau ngay trên cùng một bộ thủ tục, và nghịch lý rằng kiểm tra chặt hơn đồng nghĩa hàng đến muộn hơn đã xuất phát từ đây.

Chợ điện tử mà e-points mở ra được gọi là Brave1 Market. Một đơn vị nhận điểm theo tỷ lệ với kết quả được xác nhận qua video. Khi đơn vị đó dùng số điểm ấy để chọn drone từ một nhà sản xuất mà chính họ đã thử và tin tưởng, bộ sẽ trả tiền cho nhà sản xuất. Trong cấu trúc này, khách hàng của nhà sản xuất là đơn vị chiến đấu, không phải viên chức phụ trách mua sắm. Đây

là một thị trường nơi danh tiếng lan truyền giữa các đơn vị biến thành doanh thu, và sức sống còn của một công ty làm tốt sản phẩm cũng đến từ đó. Nhưng nó vẫn để lại những khoảng trống mà danh sách những thứ các đơn vị muốn mua không thể lấp đầy. Với bom lượn dẫn đường, loại vũ khí khó đánh chặn và có thể làm sụp đổ cả một trận địa, báo cáo ghi nhận rằng không có món hàng nào một đơn vị có thể mua được, dù họ tích lũy bao nhiêu điểm.

Các phương pháp xác minh ở phía cấp vốn cũng có giới hạn riêng. Ukraine và các quỹ có liên hệ với World Bank đã đưa vào cơ chế giám sát bên thứ ba và quy trình chuẩn hóa, vì khi quy mô hỗ trợ tăng lên, việc kiểm tra tùy từng trường hợp và dựa vào từng tư vấn viên riêng lẻ không còn gánh nổi sức nặng đó. Kiểm soát sau khi sự việc đã diễn ra nghĩa là đối chiếu sổ sách sau khi hàng đã đến nơi, nên ngay cả khi số lượng khớp, nó vẫn không thể xác định liệu những hàng hóa ấy có đạt chất lượng mà chiến trường đòi hỏi hay không.

Báo cáo mua sắm cũng ghi lại rằng các phi công bỏ ra 5 đến 30 phần trăm mức lương hằng tháng 3,000 đô la để sửa đổi thiết bị. Nhưng chưa có tài liệu nào được thu thập cho thấy tỷ lệ ấy đã giảm hay vẫn giữ nguyên sau khi e-points và DeCenter bắt đầu vận hành. Hệ thống mới có thật sự làm nhẹ đi vấn đề cũ hay không, câu trả lời chỉ xuất hiện khi có người nhìn lại vào ví tiền của binh sĩ.

Chương 11. Mặt bên kia của cải cách: Quyền lực tập trung và trách nhiệm giải trình

Ngày 30 April 2026, một cuộc phỏng vấn với Pavlo Yelizarov, phó tư lệnh Không quân Ukraine, được đăng trên kênh YouTube của Ukrainska Pravda. Tiêu đề có ba cụm: "100 ngày của Fedorov," "mái vòm chống drone," và "sự hỗn loạn của phòng không tầm ngắn." Yelizarov so sánh việc trộn nhóm mới được đưa vào Bộ Quốc phòng với Bộ Tổng tham mưu như "dầu và nước." Cho cả hai vào cùng một bát thì chúng vẫn không hòa vào nhau. Ví dụ của ông là việc đếm radar. Nếu tính địa hình trên giấy thì bốn radar là đủ để bao phủ một thành phố, nhưng người ta lại yêu cầu mười một, không vì lý do nào khác ngoài việc bảng biên chế ghi mười một.

Bảng biên chế là một văn bản được lập trước, quy định đơn vị nào giữ thiết bị nào, bao nhiêu người, và theo số lượng nào. Văn bản này thường được soạn từ lâu trước khi chiến tranh bắt đầu, và một khi đã soạn xong thì hiếm khi được sửa. Lời cáo buộc của Yelizarov là văn bản ấy đứng cao hơn địa hình. Văn bản chốt sẵn câu trả lời trước khi phép tính được thực hiện, và thói quen ngồi vào chỗ lẽ ra phải dành cho việc cân nhắc nhu cầu.

Nguồn gốc của lời cáo buộc ấy cũng đáng được chú ý. Yelizarov là khách mời trong một chương trình phát sóng. Bộ Tổng tham mưu đã trả lời ra sao về cùng vấn đề, và trang nào của tài liệu nào thực sự ghi con số mười một, đều không có trong hồ sơ công khai. Những lời chỉ trích và bảo vệ Fedorov phần lớn lưu hành dưới hình thức này. Chúng được nêu trên sóng, bị bác lại trên sóng, rồi không để lại dấu vết tài liệu nào.

Ngoài nội dung của cải cách, tính chất của những tài liệu chống đỡ cho cải cách ấy cũng phải được xem xét. Trước khi hỏi quyền lực đang tụ lại ở đâu, trước hết phải hỏi có tư liệu nào để trả lời hay không. Mốc tham chiếu là 13 July 2026, và giữa những gì tài liệu cùng chương trình phát sóng có được đến ngày đó xác nhận với những gì nằm ngoài hồ sơ công khai, có một khoảng cách lớn.

1. Cáo buộc "mafia kỹ thuật số" là lời của ai?

Fedorov được bổ nhiệm làm bộ trưởng quốc phòng vào tháng 1 năm 2026. Hơn một tháng sau, ngày 16 tháng 2 năm 2026, kênh YouTube Dana Yarova đăng một chương trình có tựa đề "Fedorov là tấm gương của Zelensky." Chương trình nêu vấn đề về những dấu hiệu cho thấy binh sĩ bị đưa vào thẩm vấn, đồng thời đặt nghi vấn rằng chính phủ cũng có ý định tổ chức bầu cử thông qua ứng dụng Diia.

Cụm từ ấy đã mang sẵn phán xét của người viết bên trong nó. "Tấm gương" được hiểu như một lời khẳng định rằng Fedorov phản chiếu lại cùng một cách cầm quyền như Zelensky. Điều hành nhà nước qua ứng dụng, màn hình và thông báo; đặt tốc độ lên trước thủ tục; tìm cách quản lý chỉ trích thay vì chịu đựng nó, tất cả được nén vào một từ duy nhất.

Vào khoảng thời gian này, cụm từ "mafia kỹ thuật số" bắt đầu lan truyền trên một số kênh YouTube chính trị của Ukraine. Hai từ ấy nén lại mối nghi ngờ rằng những người từng làm việc cùng Fedorov từ thời ông còn ở Bộ Chuyển đổi số đã tự chia nhau các vị trí then chốt trong Bộ Quốc phòng, và rằng mua sắm vũ khí, dữ liệu chiến trường cùng các nền tảng phục vụ công dân đều đã tập trung vào tay một nhóm. Một nhân vật trong ngành công nghệ quân sự được nêu là nguồn gốc của cụm từ này, nhưng hồ sơ công khai không có tài liệu gốc nào ghi nhận người đó đã nói như vậy.

Trong hồ sơ công khai, cụm từ "digital mafia" chỉ xuất hiện như một câu được trích lại trong các chương trình phát trên YouTube. Không có tài liệu gốc nào, không có văn bản do chính người đó viết, không có bản ghi nguyên thủy của một cuộc phỏng vấn mà người đó đã trả lời, cũng không có biên bản cuộc họp nào, để có thể xác nhận những lời ấy được nói khi nào, ở đâu, và trong bối cảnh nào.

"Mafia" ví một người với một tổ chức tội phạm. Một từ càng có thể làm tổn hại nặng nề đến danh dự của ai đó, thì nền tảng bên dưới người lặp lại từ ấy càng phải chắc. Vì vậy, cụm từ này không được xem ở đây như một kết luận về sự thật, mà chỉ là tên gọi của một lời phê phán đang lưu hành. Việc cụm từ ấy đang lưu hành thì đã được xác nhận. Còn điều nó cáo buộc có đúng hay không, hồ sơ công khai dừng lại tại đó.

Tình trạng lời phê phán chỉ sống trên các chương trình phát sóng cũng hiện rõ ở phía ngược lại. Ngày 10 July 2026, kênh YouTube Fabrika Novyn (Фабрика новин), khi đưa tin về việc nội các từ chức hàng loạt, đã gọi Fedorov là "điểm sáng duy nhất của nội các." Cách chương trình dựng khung vấn đề rất gay gắt. Ban lãnh đạo quân sự, trong đó có Commander-in-Chief Syrskyi, bị mắc kẹt trong một học thuyết lỗi thời, coi binh sĩ như vật tiêu hao để đẩy xuống chiến hào; Fedorov là người đang cố dùng công nghệ để chiến đấu trong cuộc chiến; và nếu President's Office không thay thế ban lãnh đạo cũ, một mình ông cũng chỉ có thể làm được đến một mức nào đó.

Fabrika Novyn là một kênh YouTube riêng lẻ, đăng các bình luận chính trị dưới những tiêu đề gây kích động. Trong hồ sơ công khai, không có bài tường thuật nào của cơ quan truyền thông khác, không có tài liệu nội bộ quân đội, cũng không có xác minh độc lập nào để ủng hộ hoặc bác bỏ cáo buộc của chương trình này rằng ban lãnh đạo quân sự theo học thuyết "vật tiêu hao". Trong không gian công luận của Ukraine thời chiến, ý đồ chính trị nhằm dựng một nhân vật lên và kéo một nhân vật khác xuống thấm vào ngôn ngữ của các chương trình phát sóng, và câu trích dẫn này được giữ trên trang giấy như một tài liệu mang tính chất ấy.

Cùng một hệ sinh thái truyền thông gọi nhóm của Fedorov là "mafia" ở một phía, và là "hy vọng duy nhất" ở phía kia. Cả hai đều là những lời khẳng định được phát sóng, và không bên nào có tài liệu chứng minh. Hai khung nhìn ấy được đặt cạnh nhau ở đây vì phần lớn thông tin mà độc giả Hàn Quốc gặp về cải cách quốc phòng của Ukraine có đúng tính chất như vậy.

Những câu chuyện anh hùng và các thuyết âm mưu được làm từ cùng một thứ vật liệu, và cả hai lan rất nhanh mà không hề được kiểm chứng.

Bản thân Fedorov không né tránh tranh cãi. Ngày 17 tháng 6 năm 2026, tiêu đề cuộc phỏng vấn của ông với kênh YouTube PRESSING đã nêu thẳng ba việc ông phải trả lời: quan hệ của ông với Syrskyi, tin đồn ông từ chức, và các nhóm tham nhũng trong lĩnh vực quốc phòng.

Việc bộ trưởng quốc phòng của một quốc gia phải trả lời cả ba câu hỏi ấy trong một buổi, khi mới nhận chức được sáu tháng, tự nó đã là một thông tin. Nó có nghĩa là ba mối nghi ngờ đã cùng lúc lớn lên quanh ông. Rằng ông đang đối đầu với tổng tư lệnh. Rằng ông sắp rời chức. Và rằng các nhóm lợi ích bao quanh mua sắm quốc phòng đang nuốt chửng cuộc cải cách của ông, hoặc chính cuộc cải cách ấy đang tạo ra một nhóm lợi ích mới của riêng nó.

Cách ông trả lời trong các cuộc phỏng vấn khá giống nhau. Ông trả lời bằng hệ thống và dữ liệu. Một bảng xếp hạng hiệu quả chiến đấu theo từng lữ đoàn, được chấm trên nhiều hạng mục và dùng làm căn cứ phân bổ nguồn lực cũng như chọn chỉ huy. Các bài kiểm tra polygraph, tức kiểm tra bằng máy phát hiện nói dối, nhằm sàng lọc những người rò rỉ thông tin trong bộ và các cơ quan mua sắm, cùng với những người vận động hành lang cho nhà cung cấp. Và việc mua sắm đạn pháo, nơi yêu cầu về tầm bắn được đưa vào hồ sơ mời thầu để chính điều kiện dự thầu thay đổi. Đó là những ví dụ ông thường quay lại. Trong số đó, ông nói, có một biện pháp, phân phối một lượng thiết bị có thể dự báo trước cho từng lữ đoàn, mất ba tháng mới thúc đẩy được.

Các con số luôn đi kèm những ví dụ này. Có bao nhiêu nhóm xếp hạng, gói thầu đầu tiên tiết kiệm được bao nhiêu phần trăm ngân sách, giá của một quả đạn pháo riêng lẻ đã giảm đến mức nào. Những con số đó không được chép lại ở đây. Tất cả đều là lời kể của chính bộ trưởng trong các cuộc phỏng vấn phát sóng, và trong hồ sơ công khai không tìm thấy tài liệu gốc nào, không có thông báo thầu, không có hợp đồng, không có báo cáo kiểm toán, để chứng minh cho chúng.

Những con số nằm ngoài hồ sơ công khai đã được để ngoài văn bản. Nhưng khi chính người thực hiện cải cách tự cộng kết quả cải cách, công bố phép cộng đó trên sóng truyền hình hoặc phát thanh, mà không có tài liệu kiểm toán bên ngoài nào tồn tại, việc chép lại các con số ấy sẽ đặt tuyên truyền vào chỗ lẽ ra phải dành cho kiểm chứng. Bất cứ ai muốn đánh giá Bộ Quốc phòng của Fedorov tính đến tháng 7 năm 2026 đều đứng trên điều kiện đó.

Cũng phải cân nhắc liệu những thay đổi này có tạo thành sự tập trung quyền lực hay không. Ở đây không khẳng định rằng quyền lực đã tập trung, cũng không khẳng định điều ngược lại. Điều còn lại là các điều kiện cấu trúc khiến nghi ngờ về sự tập trung quyền lực trở nên hợp lý. Một bộ xử lý cùng lúc việc mua sắm vũ khí, dữ liệu chiến trường và các nền tảng hướng tới công dân. Cũng chính bộ đó tự cộng các chỉ số thành tích của mình và tự công bố chúng. Và trong hồ sơ công khai không có kiểm toán độc lập hay điều tra báo chí nào để có thể kiểm tra phép cộng

ấy.

Khi ba yếu tố đó chồng lên nhau, rất khó ngăn những người chỉ trích dùng một từ xấu xí như "mafia." Điều đó không có nghĩa từ ấy là đúng. Nó có nghĩa là không có gì để bác lại nó ngoài các lời giải thích của chính bộ này. Quyền lực trên thực tế có đang bị lạm dụng hay không, và có tồn tại cơ chế nào để xác nhận hoặc phủ nhận sự lạm dụng ấy hay không, là hai câu hỏi khác nhau; chỉ câu hỏi thứ hai mới có thể nắm bắt được qua hồ sơ công khai.

Lần theo lời phê phán về tận nguồn, đôi khi người phê phán lại có lợi ích riêng. Người được nêu là nguồn gốc của cụm từ ấy làm việc trong ngành công nghiệp công nghệ quân sự. Các quy định đấu thầu và thủ tục mua sắm mà Fedorov động tới ảnh hưởng trực tiếp đến doanh thu của ngành này. Dù vậy, chưa có hồ sơ gốc nào được tìm thấy cho thấy bối cảnh người đó thực sự nói những lời ấy. Vì thế, cuốn tiểu sử này không quy cụm từ ấy cho bất kỳ cá nhân nào như một phát ngôn đã được xác lập.

Tính chất trong các câu trả lời của ông cũng đáng được ghi nhận. Xếp hạng lữ đoàn, kiểm tra bằng máy phát hiện nói dối, thay đổi điều kiện đấu thầu, tất cả đều là những cơ chế để một bộ tự nhìn vào bên trong mình. Điều vắng mặt trong hồ sơ công khai là cách các cơ quan đứng bên ngoài bộ và nhìn vào bên trong, như cơ quan kiểm toán, điều tra viên chống tham nhũng, ăn khớp với cuộc cải cách này ra sao. Những tổ chức tự kiểm tra mình thường cũng tự cho mình qua.

Các quy định mới cần bao lâu để bám rễ là một giới hạn khác. Nhận xét của ông rằng một biện pháp duy nhất, phân bổ số lượng có thể dự đoán cho từng lữ đoàn, đã mất ba tháng, cho thấy tốc độ một quyết định đi vào bên trong Ministry of Defense. Mọi nỗ lực đưa ra phán quyết về tranh chấp này khi ông mới nhậm chức được sáu tháng đều được thực hiện khi tư liệu vẫn còn thiếu.

2. Sự va chạm giữa các quyền trong chế độ nghĩa vụ quân sự, giám sát và việc nhổ tận gốc tham nhũng

TCC la viet tat cua cac trung tam tuyen quan lanh tho cua Ukraine. Day la nhung co quan tim kiem va trieu tap nhung nguoi thuoc dien dong vien. Khi chien tranh keo dai, cai ten nay da tro thanh mot trong nhung ten goi bi ghe ghet nhat trong xa hoi Ukraine.

Ngay 24 April 2026, mot chuong trinh phat thanh cua Radio NV ve cuoc cai to ma Fedorov dang soan thao da dua len tieu de y dinh cua ong muon thay doi toan bo he thong dong vien chay qua cac TCC. Cot loi cua cuoc cai cach nay giong voi cong viec ong tung lam tai Ministry of Digital Transformation. Mot phan la so hoa ho so: dua vao du lieu cac ho so cua binh si tung bi xep vao dien vang mat trai phep vi mot tai lieu giay bi that lac hoac khong duoc chuyen tu don vi nay sang don vi khac. Vang mat trai phep duoc viet tat trong tieng Ukraine la СЗЧ, co nghia la tinh trang roi khoi don vi cua minh ma khong co phep. Da co chuyen mot to giay bien mat khien

mot binh si bi gan nhan nhu vay. Phan con lai la dua vao mo hinh hop dong: ghi ro trong van ban thoi han phuc vu keo dai bao lau, va trong nhung dieu kien nao mot binh si co the chuyen sang don vi khac hoac duoc giai ngu.

Chan doan cua ong la viec tom nguoi ngoai duong roi dua len xe tai khong the tiep dien, va trong mot cuoc phong van, ong da phe phan cach lam do bang nhung tu ngu gan voi buon nguoi.

Tinh den ngay tham chieu 13 July 2026, cuoc cai to dong vien nay duoc xac nhan la ke hoach cua bo truong va la huong di ma ong da neu tren cac chuong trinh phat thanh. Khi nao no duoc ghi vao luat, duoc thuc thi den muc nao, va viec dong vien co that su thay doi vi dieu do hay khong, ho so cong khai dung lai o day. Ke hoach khong duoc chep lai nhu ket qua.

Trên thực địa, các cuộc va chạm đã xảy ra. Trong chương trình phát sóng ngày 10 July 2026, Fabrika Novyn đưa tin về một cuộc đối đầu thân thể giữa nhân viên TCC và các thanh niên ở Lviv, cáo buộc rằng nhân viên TCC đã trở thành một nhóm đặc quyền, không bao giờ ra tiền tuyến mà lại dùng bạo lực với dân thường ở hậu phương mà không bị trừng phạt. Như đã nói, kênh này chỉ là một kênh YouTube bình luận chính trị riêng lẻ, và trong hồ sơ công khai không có hồ sơ điều tra hay tài liệu tòa án nào có thể xác nhận diễn biến sự việc.

Trách nhiệm cũng bị chằng chịt. Chuỗi chỉ huy của các TCC nối với Ministry of Defense đến đâu, hồ sơ công khai dừng lại ở đó. Điều được xác nhận là cơn giận quanh việc huy động quân đang nhắm vào bộ trưởng quốc phòng, và Fedorov, thay vì lùi về sau câu hỏi thẩm quyền, đã chọn nhận lấy vấn đề. Lựa chọn ấy nguy hiểm theo hai hướng. Nếu thất bại, ông phải mang thất bại của người khác. Nếu thành công, dữ liệu huy động binh sĩ sẽ tụ về bộ của ông.

Đưa hồ sơ huy động quân sang dạng số làm hành chính nhanh hơn, nhưng cũng làm tăng rủi ro đối với quyền của công dân. Sẽ có ít người bị gắn nhãn đào ngũ hơn chỉ vì một tờ giấy bị thất lạc. Khi ngày giải ngũ được ghi cố định trong một văn bản, người lính có thể nhìn thấy trước thời gian của mình, và nghĩa vụ quân sự mà người ta có thể dự liệu cũng chính là một quyền. Nhưng cùng hệ thống ấy tạo ra một nhà nước biết vị trí, lịch sử phục vụ và di chuyển của từng công dân chi tiết hơn trước rất nhiều. Thiết bị đem lại tiện lợi và thiết bị cho phép giám sát thường là cùng một vật, và nói rằng ứng dụng cho người lính biết ngày giải ngũ chỉ là nửa đầu của câu; nửa sau là nhà nước biết tình trạng của người lính ấy theo thời gian thực.

Áp lực thu hẹp quyền cũng xuất hiện dưới những hình thức thẳng tay hơn. Yelizarov, người đã xuất hiện ở phần trước, lập luận trong cuộc phỏng vấn với Ukrainska Pravda rằng những người không đi bảo vệ đất nước có thể vẫn là công dân, nhưng không nên được phép bỏ phiếu trong các cuộc bầu cử trong mười năm tới. Chính ông thừa nhận rằng quan điểm này bị phê phán là tước bỏ một quyền hiến định, và ông không rút lại.

Đây là lập luận của một khách mời, và trong hồ sơ công khai không có căn cứ nào để gọi nó là chính sách của chính phủ. Nhưng việc một lập luận như vậy xuất hiện không chút ngần ngại trong một cuộc phỏng vấn với một cơ quan truyền thông lớn cho thấy không gian công cộng thời chiến đã bắt đầu đặt những quyền cơ bản như phổ thông đầu phiếu lên bàn mặc cả. Phổ thông đầu phiếu là quyền mà một người có vì là công dân. Khoảnh khắc nó bị biến thành phần thưởng trao cho những người đã lập công, nó đã trở thành một thiết chế khác, và nguyên tắc ấy đang lung lay trước lý lẽ biện minh của chiến tranh.

Sự nghi ngờ về bầu cử cũng đi theo hướng ngược lại. Chương trình phát sóng của Dana Yarova nêu cáo buộc rằng chính phủ có ý định tổ chức bầu cử thông qua ứng dụng Diia. Một khi một ứng dụng đang giữ giấy tờ định danh và dịch vụ hành chính cũng giữ cả việc bỏ phiếu, một số câu hỏi sẽ lập tức xuất hiện. Số phận của những người không thể truy cập ứng dụng sẽ ra sao. Ai kiểm chứng việc kiểm phiếu. Điều gì ngăn được sự ép buộc từ nơi làm việc hoặc từ một đơn vị yêu cầu bạn mở ứng dụng và cho họ xem. Một trong những điều mà lá phiếu giấy từng bảo vệ là bí mật. Hồ sơ công khai không có văn bản chính phủ nào ủng hộ cáo buộc này, cũng không có kiểm chứng độc lập nào bác bỏ nó; điều được xác nhận chỉ là sự nghi ngờ ấy đang tồn tại.

Bộ Chuyển đổi Số đã đáp lại những nghi ngờ kiểu này bằng văn bản. Ngày 30 June 2026, bộ này ban hành một tuyên bố chính thức phản hồi các "tuyên bố thao túng" về Diia City, cơ chế dành cho các công ty IT mà bộ đã quảng bá. Văn bản đó là lời tự biện hộ do chính bộ viết cho mình. Việc không thể nghe lời phê phán bằng chính tiếng nói của người phê phán, mà chỉ biết đến nó qua phần tóm lược trong một văn bản phản bác, tự nó đã là một sự lệch nền tảng. Những báo cáo mà xã hội dân sự và các tổ chức nhân quyền của Ukraine đã công bố về Diia và việc số hóa nghĩa vụ quân sự, các tài liệu ấy không thể thu thập được. Lấp khoảng trống đó rồi viết rằng "những lo ngại đã bị phóng đại" sẽ là đối xử với một thông cáo của chính phủ như thể nó có cùng trọng lượng với kiểm chứng.

Các công cụ giám sát đã trở thành một phần của chiến tranh. Ukraine đã dùng công nghệ của Clearview AI, công ty nhận diện khuôn mặt của Mỹ, ngay từ những ngày đầu của cuộc chiến. Nhận diện khuôn mặt chuyển các đặc điểm của một khuôn mặt trong ảnh thành các con số, rồi đối chiếu chúng với một cơ sở dữ liệu khuôn mặt khổng lồ đã được tập hợp sẵn để xác định một người. Hệ thống này được cho là đã nhận diện hơn 230,000 binh sĩ Nga và đã được dùng để truy vết tội ác chiến tranh. Chính công ty đó đã bị phạt nặng ở Pháp, Italy và các nước châu Âu khác vì xây dựng cơ sở dữ liệu của mình bằng cách thu thập hàng tỷ bức ảnh từ mạng xã hội mà không có sự đồng ý. Công cụ phơi bày tội ác chiến tranh và công cụ bị phán là trái luật ở châu Âu là cùng một công cụ, và sự cấp bách của chiến tranh xóa đi những ranh giới mà luật thời bình đã vạch ra.

Bên trong các thành phố, tình hình cũng gần như vậy. Kyiv và các thành phố lớn khác được phủ bởi mạng lưới camera "Safe City", có nhận diện khuôn mặt và nhận diện biển số xe. Các nhóm dân sự gọi đó là "con mắt sắc bén của Big Brother" và cảnh báo về việc giám sát đời sống riêng tư. Tháng 3 năm 2022, quốc hội thông qua một đạo luật (No. 2123-XI) cho phép cảnh sát truy cập các cơ sở dữ liệu sinh trắc học, gồm dấu vân tay và dữ liệu khuôn mặt. Các tổ chức nhân quyền cảnh báo rằng việc thu thập thông tin sinh trắc học mà không có biện pháp bảo vệ sẽ để lại một vết thương không thể đảo ngược.

Cụm từ "không thể đảo ngược" cần được hiểu đúng theo nghĩa đen. Dấu vân tay và khuôn mặt không phải là mật khẩu. Mật khẩu bị lộ có thể đổi được; dấu vân tay thì không. Và những gì chiến tranh biện minh sẽ còn ở lại sau khi chiến tranh kết thúc. Camera không bị tháo xuống, cơ sở dữ liệu không bị xóa. Mạng lưới giám sát này không phải là thứ Fedorov đích thân khởi xướng, nhưng nó vận hành trên hệ thống hạ tầng nhà nước mà ông đã đặt nền.

Quyền cá nhân cũng có thể bị xâm phạm trong quá trình điều tra tham nhũng và cải cách hành chính. Việc Fedorov thúc đẩy kiểm tra bằng máy phát hiện nói dối trên diện rộng trong Bộ Quốc phòng và các cơ quan mua sắm ngay sau khi nhậm chức là điều chính ông đã nói trong các cuộc phỏng vấn. Ông nói rằng cả những người từ chối kiểm tra lẫn những người không vượt qua bài kiểm tra đều mất chức.

Mục tiêu nhổ tận gốc tham nhũng là chính đáng. Khi tiền dùng để mua vũ khí bị thất thoát, binh sĩ ngoài mặt trận phải chết. Nhưng máy phát hiện nói dối chỉ đo các phản ứng cơ thể được cho là xuất hiện khi một người nói dối, như thay đổi nhịp tim, mồ hôi, hơi thở, chứ không thể đọc được chính lời nói dối. Độ chính xác của nó đã bị tranh cãi trong thời gian dài, và tòa án ở nhiều nước không chấp nhận kết quả này làm chứng cứ. Một thủ tục sa thải công chức dựa trên kết quả kiểm tra hoặc việc từ chối kiểm tra, không có cáo trạng và không có xét xử, va chạm trực diện với nguyên tắc tố tụng đúng luật. Việc này được thực hiện trên cơ sở pháp lý nào, có ai nộp đơn phản đối hay không, và kết quả ra sao, đến đây hồ sơ công khai dừng lại.

Việc dùng quyền lực nhà nước để đối phó với người chỉ trích cũng đã nổi lên như một vấn đề. Theo chương trình phát sóng của Dana Yarova, doanh nhân Ihor Kryvetskyi, người công khai chỉ trích chính sách của bộ khi cho rằng việc trưng binh nam giới từ 18 đến 24 tuổi chẳng khác nào phá hủy lực lượng dự bị, sau đó đã bị Cơ quan An ninh Ukraine (SBU) khám xét xe trên đường và nhận giấy triệu tập vì bị nghi cản trở hoạt động hợp pháp của lực lượng vũ trang Ukraine. Đây cũng chỉ là tường thuật của một kênh, và trong các tài liệu công khai không có hồ sơ điều tra hay xác nhận độc lập từ một cơ quan truyền thông khác. Nhưng nếu việc đó là thật, nó có nghĩa là ngưỡng để coi việc chỉ trích chính sách quân sự là tội cản trở hoạt động quân sự đã bị hạ xuống. Khi ranh giới giữa chỉ trích chính sách và giúp kẻ thù trở nên mờ đi, người ta nói ít hơn, và phần còn lại là im lặng.

Gốc rễ của vấn đề này sâu hơn bất kỳ một cá nhân nào. Vào tháng 7 năm 2025, trước khi Fedorov trở thành bộ trưởng quốc phòng, một dự luật (dự thảo số 12414) đã được đưa ra trước quốc hội Ukraine, và trên thực tế có thể đã tháo dỡ tính độc lập của Cục Chống Tham nhũng Quốc gia (NABU) và Văn phòng Công tố Chống Tham nhũng Chuyên trách (SAPO). Đây là các cơ quan điều tra và truy tố tham nhũng của quan chức cấp cao. Sự phản ứng tức thời từ xã hội dân sự, trong đó có Anti-Corruption Action Center, đã giữ được tính độc lập của hai cơ quan này.

Đã có một nỗ lực từ những người nắm quyền nhằm kiểm soát các cơ quan theo dõi tham nhũng, và lực lượng ngăn chặn nỗ lực đó đến từ sự phản kháng của xã hội dân sự. Tình tiết này là một tọa độ cần đặt ở nền sau khi đọc về cải cách của Fedorov. Ở Ukraine, các cơ chế kiểm soát quyền lực chỉ vừa đủ được giữ lại nhờ những người xuống đường, và thực trạng một bộ nắm quyền lực lớn trong thời chiến phải chịu sự kiểm soát vốn đã yếu ngay từ đầu vẫn còn đó, bất kể cuộc cải cách rồi sẽ đi đến đâu.

Hãy bắt đầu từ quy mô của vấn đề. Fedorov nói trong một chương trình phát sóng rằng khoảng hai triệu người đang bị truy tìm để trưng binh và hơn 200.000 binh sĩ được xếp vào diện vắng mặt không phép. Những con số này đến từ chính bộ trưởng, và trong hồ sơ công khai không có công bố của cơ quan thống kê hay tài liệu kiểm toán nào xác nhận chúng. Dù các con số không thật chính xác, hoàn cảnh vẫn còn đó: một hệ thống trong đó một tờ giấy có thể thay đổi tình trạng của một con người đang vận hành ở quy mô hàng trăm nghìn người.

Về câu hỏi trách nhiệm, phía bộ trưởng có cách giải thích riêng. Các TCC không thuộc Bộ Quốc phòng mà thuộc Lục quân, nhưng các chính trị gia vẫn dùng chúng như một cây gậy để đánh vào ông. Trong hồ sơ công khai không có sơ đồ tổ chức hay đạo luật nào xác nhận cách giải thích này. Dù các đơn vị ấy thuộc về đâu, cơn giận vẫn đổ về phía bộ trưởng quốc phòng.

Dự luật số 8153 là dự luật bảo vệ dữ liệu cá nhân được trình vào tháng 10 năm 2022. Giống GDPR của Liên minh châu Âu, dự luật này có quyền truy cập và xóa dữ liệu, giảm thiểu việc thu thập, và bảo vệ thông tin sinh trắc học. Trong khi yêu cầu phải có sự đồng ý của cá nhân khi xử lý dữ liệu sinh trắc học, dự luật lại cho phép rõ ràng các cơ quan điều tra lắp đặt camera giám sát ở nơi công cộng. Dự luật cũng thiết lập quyền chung được từ chối xử lý tự động, nhưng không phân tầng mức độ rủi ro của việc dùng AI. Các điều khoản bảo vệ và ngoại lệ giám sát cùng nằm trong một dự luật, và các tổ chức nhân quyền yêu cầu những cơ chế kiểm soát phải được viết cụ thể hơn.

3. Làm thế nào để giữ trách nhiệm giải trình trong một cuộc chiến công nghệ tốc độ cao

Máy móc ra phán đoán càng nhanh, việc xác định ai chịu trách nhiệm cho một quyết định sai càng dễ trở nên mờ nhạt. Số thứ hai của tạp chí chính sách quân sự Hoa Kỳ Modern War Journal trả lời câu hỏi này bằng những câu ngắn và rắn. Tạp chí viết rằng đổi mới tự nó không có nghĩa

là lợi thế; công nghệ không có học thuyết sẽ sinh ra điểm yếu, tốc độ không có phán đoán sẽ kéo theo rủi ro chiến lược, và tự chủ không có trách nhiệm giải trình sẽ phá hủy niềm tin, nền tảng của nghề quân nhân.

Ba cặp khái niệm hiện ra. Công nghệ và học thuyết, tốc độ và phán đoán, tự chủ và trách nhiệm giải trình. Học thuyết nghĩa là các quy tắc của quân đội về khi nào và bằng cách nào một vũ khí được dùng; trách nhiệm giải trình nghĩa là nguyên tắc rằng người đưa ra quyết định phải giải thích và gánh chịu kết quả. Nếu chỉ giữ vế đầu của mỗi cặp và rút rỗng vế thứ hai, thứ còn lại là một quân đội sai rất nhanh.

Tốc độ có thể đi xa đến đâu đã được chứng minh trên một chiến trường khác. Cũng tạp chí đó ghi nhận rằng Gospel, hệ thống đề xuất mục tiêu mà Israel dùng ở Gaza, rà soát mục tiêu và đưa ra khuyến nghị tấn công nhanh hơn ít nhất năm mươi lần so với một nhà phân tích con người. Năm mươi lần là tốc độ không ai có thể theo kịp, và nói rằng con người không thể theo kịp cũng đồng nghĩa với nói rằng con người không thể kiểm tra. Người phê chuẩn mà không kiểm tra thì chỉ đang bấm một nút.

Vì vậy, các tài liệu chính sách đã đóng đinh vai trò của trí tuệ nhân tạo. Một báo cáo của IFRI, chắt lọc cuộc chiến công nghệ quân sự thành tám bài học, định nghĩa AI là một "bộ tăng tốc quy trình" và không đặt nó vào chiếc ghế của vị chỉ huy ra quyết định. Nó là công cụ lục tìm hàng nghìn giờ hình ảnh từ drone và ảnh vệ tinh để tập hợp rồi đưa các mục tiêu ứng viên lên trước mắt; là công cụ đỡ lấy một chỉ huy đã nhiều ngày không ngủ để năng lực phán đoán của người đó không cạn kiệt. Khi chưa có khung pháp lý nào xác định trách nhiệm của một cỗ máy, báo cáo viết, AI không được trở thành một hệ thống thay thế thẩm quyền của con người.

Học thuyết quân sự gọi nguyên tắc này là Human-in-the-Loop. Nó có nghĩa là con người luôn phải nằm trong vòng lặp của bất kỳ quyết định nào có thể giết một người. Modern War Journal viết rằng chưa có bằng chứng cho thấy bất kỳ quốc gia nào đã triển khai một hệ thống vũ khí AI trong chiến đấu mà không giữ con người trong vòng lặp. Đó là sự xác nhận rằng vẫn còn một ranh giới chưa bị vượt qua; nhưng nó không bảo đảm rằng ranh giới ấy sẽ được giữ vững.

Có một hướng nghiên cứu giúp giải thích vì sao con người vẫn phải được giữ lại, nếu nói theo một cách khác. Bài "Prediction and Judgment" của Avi Goldfarb và Jon Lindsay lập luận rằng trí tuệ nhân tạo trên thực tế làm vai trò của con người trong chiến tranh trở nên quan trọng hơn. Điều AI làm tốt là dự đoán: tìm ra mô thức trong dữ liệu và đoán điều gì sẽ xảy ra tiếp theo. Phán đoán, tức cân nhắc dự đoán ấy có ý nghĩa gì trong bối cảnh chính trị và quân sự hiện tại, việc tấn công mục tiêu này nói lên điều gì đối với toàn bộ cuộc chiến, vẫn là phần việc của con người. Khi dự đoán càng rẻ và càng dồi dào, cái giá của phán đoán càng tăng.

Vấn đề là liệu con người có còn tiếp tục đưa ra phán đoán ấy được hay không. Khi máy móc đưa ra một câu trả lời nghe có vẻ hợp lý, việc nghi ngờ nó đòi hỏi công sức. Không nghi ngờ bao giờ cũng nhanh hơn, và trong thời chiến, nhanh thường trông giống đúng.

Điều mà Bộ Quốc phòng của Fedorov đưa ra làm tiêu chuẩn là tốc độ. Tốc độ mua sắm, tốc độ phân phối, tốc độ đưa phản hồi từ tiền tuyến quay trở lại sản xuất. Nhìn vào những ví dụ ông nêu trên các chương trình phát sóng, ngay cả câu nói rằng một biện pháp mất ba tháng mới được thông qua cũng xuất hiện như một lời khoe. Nghe như ông đang nói rằng trước đây, một biện pháp như thế thậm chí sẽ chẳng bao giờ được thông qua.

Những gì đã được xác lập trước đó lại là một danh sách ở phía đối diện. Các con số về hiệu suất do chính bộ này cộng lại. Trong hồ sơ công khai không có tài liệu kiểm toán bên ngoài nào để kiểm tra khoản tiết kiệm từ cải cách mua sắm. Phản bác của Bộ Tổng tham mưu chưa từng được ghi nhận. Không thể biết những người mất chức vì kiểm tra bằng máy phát hiện nói dối đã đưa khiếu nại của họ tới đâu, và dù có bài báo nói rằng một công dân chỉ trích chính sách của bộ đã bị Cơ quan An ninh triệu tập, cũng không có tài liệu nào để xác nhận đầy đủ diễn biến của vụ việc đó.

Buộc quyền lực phải chịu trách nhiệm đòi hỏi ba cơ chế cùng vận hành: công bố hồ sơ, kiểm toán độc lập và kiểm soát của quốc hội. Nói cách khác: phải có hồ sơ, phải có kiểm chứng, và phải có chỗ để phản đối. Căn cứ của một cuộc tấn công phải được lưu lại trong hồ sơ; một người không phải là người đã lập bảng tính phải kiểm tra lại; và những người bị thiệt hại cũng như những người lên tiếng phê phán phải có một kênh để nói. Tính đến ngày 13 July 2026, trong hồ sơ công khai, ba chức năng ấy tại Ministry of Defense của Fedorov hoặc đang trống, hoặc do chính bộ này tự lấp đầy.

Bài viết của Jere Perez trên Modern War Journal lật câu hỏi theo hướng khác. Ông viết rằng các hệ thống tự chủ sẽ không phải là thứ quyết định bên nào nắm lợi thế trên chiến trường tương lai. Chính những con người được tin cậy đến mức được giao các hệ thống ấy mới quyết định điều đó. Ông kết lại bằng một câu rằng lợi thế quyết định không đến từ việc một quân đội đưa loại trang bị nào ra chiến trường, mà đến từ việc quân đội ấy đào tạo nên kiểu con người nào.

Fedorov đã bắt tay vào thay đổi một tổ chức quân sự cũ và các thủ tục mua sắm của nó. Dữ liệu thay cho giấy tờ, chỉ số thay cho họp hành, đấu thầu thay cho lệ cũ. Cuộc đấu ấy có lý lẽ của nó, và những người lính ngoài mặt trận rất có thể đã nhận được lợi ích thật từ đó.

Nhưng một trong những việc mà bảng biên chế cũ đã làm là buộc thẩm quyền phải gắn với một văn bản. Chính văn bản buộc phải nêu yêu cầu về eleven radar cũng là văn bản ngăn bất kỳ ai tùy hứng biến eleven thành twenty. Chậm chạp và bị ràng buộc thường đi cùng một thân thể; và nơi lệ cũ đã bị dọn đi, khoảng trống do chiếc phanh mà lệ cũ từng cung cấp để lại cũng còn nằm đó.

Văn bản có thể ràng buộc thứ quyền lực nay đã chuyển vào dữ liệu vẫn chưa được viết ra. Ai sẽ viết nó? Tính đến ngày 13 July 2026, chưa có văn bản công khai nào đưa ra câu trả lời.

How leaning on algorithms eats away at command được Adam Ropelewski viết trên cùng tạp chí. Cứ dựa vào khuyến nghị của máy móc hết lần này đến lần khác, quyền chủ động hành động trước của người chỉ huy sẽ co lại, còn độ linh hoạt của mission command cũng bị gọt mỏng dần. Mission command nghĩa là chỉ giao mục tiêu, rồi để người chỉ huy tại hiện trường tự quyết định cách làm, thay vì cấp trên chỉ đạo từng bước. Khi máy móc đưa câu trả lời ra trước, hiện trường không còn gì để tự quyết nữa.

Cuộc trò chuyện giữa General Votel và Dean Reeves trên cùng tạp chí đã đặt tên cho cám dỗ ấy. Đẩy dữ liệu vào máy, một kết quả nghe có vẻ hợp lý sẽ đi ra, rồi người ta bắt đầu muốn giao luôn việc quyết định cho máy, thay vì tự mình làm việc đó. Reeves nói các thiết bị điện tử đã làm sức tập trung của con người ngắn lại, và trong trạng thái ấy, kiểu suy nghĩ sâu cần có để xuyên qua sự bất định của chiến tranh không xuất hiện. Bài rèn luyện mà ông tự đặt ra cho mình là cất các thiết bị đi, rồi đọc trọn một tờ báo giấy và một cuốn sách lịch sử dày. Nghĩa là trở thành một người không đông cứng khi máy móc đẩy một kết luận ra trước mặt, một người có thể tự nghĩ ra lối thoát của mình.

Đây là lý do Perez lần theo vấn đề đến tận khâu tuyển mộ. Quyền tự chủ không được ban xuống từ trên; nó đến từ bản sắc được hình thành ngay ở điểm tiếp xúc đầu tiên với quân đội. Trong hồ sơ công khai, cuộc cải cách của Fedorov nói về mua sắm, dữ liệu và hợp đồng. Còn về cách nuôi dưỡng những con người không buông bỏ phán đoán trước máy móc, hồ sơ công khai dừng lại ở đó.

Kết luận. Trạng thái bình thường mới của chiến tranh số trong thế kỷ XXI

Sự nghiệp của Mykhailo Fedorov bắt đầu từ một màn hình duy nhất rồi đi thẳng vào bên trong Ministry of Defence. Diia đã đưa cánh cửa hành chính công lên điện thoại thông minh, và sau cuộc xâm lược, viện trợ sơ tán, báo cáo thiệt hại, cùng thông tin thời chiến đều đi qua cánh cửa ấy. Starlink cho thấy một công ty nằm ngoài mạng viễn thông quốc gia vẫn có thể nắm trong tay đường kết nối của cả một cuộc chiến. IT Army để lại một khoảng trống trong luật pháp và chỉ huy, nằm giữa lời kêu gọi của chính phủ và các cuộc tấn công do tình nguyện viên ở ngoài biên giới phát động. Brave1 và các chương trình drone cho thấy điều gì xảy ra khi start-up, quyên góp, mua sắm công và chiến đấu cùng vận hành trong một mạch khép kín.

Sức mạnh của mạch ấy là tốc độ. Một nhu cầu từ tiền tuyến đến được với các nhà phát triển, và thời gian để một mẫu thử vượt qua kiểm tra rồi tới một đơn vị chiến đấu ngày càng ngắn lại. Dữ liệu đi ngược lên theo chuỗi chỉ huy thay cho báo cáo giấy, và nhiều nỗ lực lặp đi lặp lại đã được thực hiện để nối đơn đặt hàng thiết bị với hiệu quả trên chiến trường. Khó có thể phủ nhận rằng một quốc gia đang ở giữa chiến tranh đã cố thay đổi trong vài tháng những việc thông thường phải mất nhiều năm mới cải cách được.

Ở phía bên kia của tốc độ là trách nhiệm giải trình. Điều khoản dịch vụ của một công ty tư nhân phân chia phạm vi hoạt động, các cuộc tấn công của tình nguyện viên hòa lẫn vào hành động của nhà nước, và chính phủ đánh giá hiệu quả của những công ty mà chính mình đã tài trợ. Ngay cả khi dữ liệu khiến quyết định được đưa ra nhanh hơn, những gì dữ liệu bỏ sót không tự hiện ra. Kiểm toán, giám sát của nghị viện, và các thủ tục bảo vệ quyền của công dân trông có vẻ chậm chạp khi nhìn từ chiến trường, nhưng khi các thủ tục ấy biến mất, trách nhiệm đối với thất bại cũng mờ đi cùng chúng.

Fedorov mang gương mặt của một nhà cải cách và gương mặt của một nhà quản trị đã gom quyền lực về tay mình. Ông khiến một bộ máy chính phủ cũ kỹ chuyển động nhanh hơn, và trong quá trình đó ông vẽ lại ranh giới giữa chính phủ và doanh nghiệp, giữa công dân và quân đội. Câu hỏi trung tâm là ai sẽ theo dõi đường ranh ấy. Tính đến 13 July 2026, các thiết chế công vẫn chưa trả lời thỏa đáng câu hỏi đó.

Chiến tranh thử thách công nghệ, nhưng nó không cho phép nền dân chủ được miễn trách nhiệm giải trình. Hồ sơ tiếp theo về nhiệm kỳ của Fedorov sẽ không chỉ được viết bằng sản lượng drone hay số người dùng ứng dụng. Liệu nhà nước vận hành nhanh mà ông xây dựng có chịu được phê bình, công khai sổ sách và chia sẻ thẩm quyền hay không, kết quả ấy sẽ quyết định sức nặng của những chương còn ở phía trước.

1. Thư mục

Tất cả URL đã được kiểm tra vào ngày 13 July 2026.

Navigating Ukraine's Defense Tech Market. EY, 2025-10-01.

https://www.ey.com/content/dam/ey-unified-site/ey-com/en-ua/insights/defense-tech/navigating-ukraine-defense-tech-market.pdf

Ukraine: Sức bền kỹ thuật số trong thời chiến. Brookings Institution, 2024-01-01.

https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf

Những bài học từ cuộc chiến tranh mạng đầu tiên. Henry Jackson Society, 2024-02-01.

https://henryjacksonsociety.org/wp-content/uploads/2024/02/Lessons-from-the-First-Cyberwar-by-Kirichenko.pdf

Drones trong chiến tranh hiện đại: Những bài học rút ra từ cuộc chiến ở Ukraine. Australian Army Research Centre, 2024-10-22.

https://researchcentre.army.gov.au/sites/default/files/241022-Occasional-Paper-29-Lessons-Learnt-from-Ukraine_2.pdf

Drones tự hành: Các xu hướng mới nổi từ Ukraine. CAPSS India, 2026-02-01.

https://capssindia.org/wp-content/uploads/2026/02/8-Abhishek-Kumar.pdf

Cuộc chiến của Nga tại Ukraine: Một năm hoạt động mạng. CERT-EU, 2023-02-01.

https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Lập bản đồ cuộc chiến MilTech: Tám bài học từ chiến trường Ukraine. IFRI / Munich Security Conference, 2026-02-01.

https://securityconference.org/assets/01_Bilder_Inhalte/05_Marketplace_of_Ideas/MSC_2026/ifri_tenenbaum_et_al_miltech_war_ukraine_2026_0.pdf

Những diễn biến trong quản trị không gian và tác động của cuộc chiến ở Ukraine. SIPRI, 2023-06-01.

https://www.sipri.org/sites/default/files/SIPRIYB23c11sIII.pdf

Tăng cường khả năng chống chịu bằng cách thúc đẩy chuyển đổi số trong doanh nghiệp tại Ukraine. OECD, 2024-05-01.

https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf

Những diễn biến trong quản trị không gian mạng và tác động của cuộc chiến ở Ukraine. SIPRI, 2023-06-01.

https://www.sipri.org/sites/default/files/SIPRIYB23c11sIV.pdf

Sự phát triển của phòng thủ mạng Ukraine. CCDCOE, 2026-03-01.

https://ccdcoe.org/uploads/2026/03/CCDCOE_Policy_Brief_Ukraines_Cyber_Defence_Evolution.pdf

Hệ sinh thái drone của Ukraine và việc phòng vệ châu Âu. LSE IDEAS, 2025-04-05.

https://www.lse.ac.uk/ideas/Assets/Documents/Research-Reports/2025-04-05-DRONES-MatlackSchwartzGill-FINAL-WEB.pdf

Những chuyển đổi số trong hệ thống an ninh mạng của Ukraine thời chiến. ARMG Publishing, 2025-11-01.

https://armgpublishing.com/wp-content/uploads/2025/11/monograph-3-2025.pdf

Mặt trận kỹ thuật số phía Đông không hề yên ả. New Strategy Center, 2024-06-01.

https://newstrategycenter.ro/wp-content/uploads/2024/06/NOTHING-QUIET-ON-THE-EASTERN-DIGITAL-FRONT_NSC.pdf

Tận dụng năng lực sản xuất drone của Ukraine. Prism UA, 2025-04-01.

https://prismua.org/wp-content/uploads/2025/04/Blue_and_yellow_annex_on_defense.pdf

Kháng cự kỹ thuật số của Ukraine trước sự xâm lược của Nga. StrategEast, 2022-05-01.

https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf

Wizard Warfare: Tổng quan về các phát triển công nghệ của Ukraine. Johns Hopkins APL, 2025-01-01.

https://www.jhuapl.edu/sites/default/files/2025-01/WizardWarfare_final.pdf

Những bài học từ phòng thủ thông tin của Ukraine cho sức bền dân chủ. CIGI, 2025-06-01.

https://www.cigionline.org/static/documents/DPH-Paper-Padalko_Summer2025.pdf

Một thập niên trong chiến hào của chiến tranh mạng. National Security Archive, 2024-02-02.

https://nsarchive.gwu.edu/sites/default/files/documents/semon9-ryglx/2024-02-02-Cyber-Diia-A-Decade-in-the-Trenches-of-Cyberwarfare.pdf

Từ chính sách đến chiến thắng: Khai thác công nghệ quốc phòng. RAND, 2025-12-01.

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3800/RRA3833-2/RAND_RRA3833-2.pdf

Bài học từ cuộc chiến ở Ukraine cho lĩnh vực không gian. RAND, 2025-03-01.

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2950-1/RAND_RRA2950-1.pdf

Chuyển đổi số tại Ukraine. KPMG, 2025-11-01.

https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2025/11/Digital%20Transformation%20in%20Ukraine.pdf

Xây dựng và phát huy năng lực drone của Ukraine trong xung đột và cả sau đó. Murray Lab, 2025-03-01.

https://murray-lab.org/wp-content/uploads/2025/03/UkraineDroneEcosystem-Analysis_2025.pdf

Phòng thủ mạng của Ukraine. German Marshall Fund, 2023-12-01.

https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf

Ngành công nghiệp drone của Ukraine: Đầu tư và đổi mới sản phẩm. KSE Institute / Brave1, 2024-10-04.

https://kse.ua/wp-content/uploads/2024/10/241004-Brave1-report-v.1.pdf

Xây dựng tuyến đầu kỹ thuật số. Atlantic Council, 2025-11-01.

https://www.atlanticcouncil.org/wp-content/uploads/2025/11/CSI_CompaniesAtWar.pdf

Đánh giá chiến tranh mạng và chiến tranh thông tin của Nga tại Ukraine. CNA, 2023-11-01.

https://www.cna.org/reports/2023/11/Assessing-Russian-Cyber-and-Information-Warfare-in-Ukraine.pdf

Lộ trình Chuyển đổi Công nghiệp Quốc phòng EU. European Commission, 2025-12-01.

https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf

Quá trình số hóa nhanh chóng của Ukraine. CSIS, 2024-02-14.

https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-02/240214_Flacks_Ukraine_Digitalization.pdf?VersionId=_ZNBi1gSW50ffi6fn0KbZXHMDbEHR_cU

Chiến tranh mạng trong Chiến tranh Nga Ukraine: Những bài học cho Ấn Độ. CENJOWS, 2025-12-01.

https://cenjows.in/wp-content/uploads/2025/12/Flt-Lt-Shobhit-Mehta-Gp-Capt-Umang-Kumar-_-Article.pdf

Lập bản đồ cuộc chiến MilTech: Tám bài học từ chiến trường Ukraine. IFRI, 2026-02-01.

https://www.ifri.org/sites/default/files/2026-02/ifri_tenenbaum_et_al_miltech_war_ukraine_2026.pdf

Thị trường công nghệ quốc phòng Ukraine. KSE Institute, 2026-03-31.

https://institute.kse.ua/wp-content/uploads/2026/03/the-ukrainian_defense_technology_market_eng_march_2026.pdf

Sáu bài học then chốt từ cuộc chiến drone của Ukraine. Irregular Warfare Center, 2026-05-20.

https://irregularwarfarecenter.org/wp-content/uploads/I_10_Six_Key_Lessons_from_Ukraine_Drone_War.pdf

Business Ukraine Spring 2026. Business Ukraine, 2026-05-01.

https://businessukraine.ua/wp-content/uploads/2026/05/BUSINESS_UKRAINE_SPRING_2026.pdf

Enabling Ukraine's Response at Scale. World Bank, 2026-03-01.

https://documents1.worldbank.org/curated/en/099713103262663347/pdf/IDU-8f5a661b-317c-4cbb-ab7e-0a9c95156336.pdf

Báo cáo của Progressive Policy Institute về công nghệ quốc phòng Ukraine. Progressive Policy Institute, 2026-04-01.

https://www.progressivepolicy.org/wp-content/uploads/2026/04/2026_04_TJacoby_FINAL.pdf

Dronisation without militarisation. EPIK, 2026-03-01.

https://epik.eu/?ut_download=1329&ut_token=5fb94e345668040f3f9c87be282918f9

UAVs: ISR, Răn đe và Chiến tranh. IISS, 2026-03-01.

https://www.iiss.org/globalassets/media-library---content--migration/files/publications---free-files/strategic-dossier/uavs-2026/iiss_uavs-isr-deterrence-and-war_032026.pdf

Hướng tới Phòng thủ Thông minh. Cambridge Centre for Geopolitics, 2026-02-01.

https://www.cfg.cam.ac.uk/wp-content/uploads/2026/02/Towards-Smart-Defence.-Victoria-Vdovychenko-2.pdf

Teaching Humans in the Loop. LSE IDEAS, 2026-06-01.

https://www.lse.ac.uk/asset-library/matlack-j-and-gill-o-teachinghumansintheloop-1.pdf

2026 Annual Threat Assessment. ODNI, 2026-03-01.

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf

Modern War Journal, ấn bản thứ hai. Modern War Institute, 2026-03-19.

https://mwi.westpoint.edu/wp-content/uploads/2026/03/Modern-War-Journal-MWJ-second-edition-final-draft-as-of-19MAR26.pdf

Lập bản đồ nhu cầu tái thiết thời bình của Ukraine. European Parliament, 2026-07-01.

https://www.europarl.europa.eu/RegData/etudes/STUD/2026/783617/EXPO_STU%282026%29783617_EN.pdf

Cung cấp và quản lý năng lượng chiến thuật trong chiến tranh Ukraine. US Army, 2026-03-30.

https://api.army.mil/e2/c/downloads/2026/03/30/c260713f/no-26-1116-powering-the-front-tactical-energy-delivery-and-management-in-the-ukraine-war.pdf

Про призначення Федорова М.А... | від 14.01.2026 № 4756-IX [Về việc bổ nhiệm M. A. Fedorov | 14 tháng 1 năm 2026, số 4756-IX]. Verkhovna Rada of Ukraine, 2026-01-14.

https://zakon.rada.gov.ua/laws/show/4756-20

Сьогодні ми почали суттєве перезавантаження - зміни внутрішні, щоб Україна була більш стійкою - звернення Президента [Hôm nay chúng ta đã bắt đầu một cuộc tái khởi động đáng kể, những thay đổi nội bộ để Ukraine trở nên bền bỉ hơn: bài phát biểu của Tổng thống] - Văn phòng đại diện chính thức trên Internet của Tổng thống Ukraine. President of Ukraine, 2026-01-13.

https://www.president.gov.ua/news/sogodni-mi-pochali-suttyeve-perezavantazhennya-zmini-vnutris-102277

Mykhailo Fedorov được bổ nhiệm làm Bộ trưởng Quốc phòng mới của Ukraine | MoD News. Ministry of Defence of Ukraine, 2026-01-14.

https://mod.gov.ua/en/news/mykhailo-fedorov-appointed-as-ukraine-s-new-minister-of-defence

Mykhailo Fedorov ký lệnh khởi động hệ thống chỉ huy và kiểm soát drone Mission Control trong DELTA | Tin tức MoD. Ministry of Defence of Ukraine, 2026-01-23.

https://mod.gov.ua/en/news/mykhailo-fedorov-signs-order-to-launch-mission-control-drone-command-and-control-system-in-delta

Понад 75 млн доларів внесків та оголошення набору до Армії дронів: UNITED24 звітує про два місяці роботи [Hơn 75 triệu USD tiền đóng góp và thông báo tuyển quân vào Army of Drones: UNITED24 báo cáo về hai tháng hoạt động]. UNITED24, 2022-07-01.

https://u24.gov.ua/uk/news/reports_on_two_months_of_activity

Михайло Федоров: Армію дронів посилять ударні БПЛА українського виробництва. Підписали контракти про співпрацю з чотирма компаніями [Mykhailo Fedorov: Lực lượng

Army of Drones sẽ được tăng cường bằng các UAV tấn công do Ukraine sản xuất. Các hợp đồng hợp tác đã được ký với bốn công ty]. Ministry of Digital Transformation of Ukraine, 2022-10-30.

https://thedigital.gov.ua/news/army/mikhaylo-fedorov-armiyu-droniv-posilyat-udarni-bpla-ukrainskogo-virobnitstva-pidpisali-kontrakti-pro-spivpratsyu-z-chotirma-kompaniyami

Cụm công nghệ quốc phòng Brave1. Brave1, 2026-07-13.

https://brave1.gov.ua/en/

Diia - thông tin về dự án Diia. Digital State UA, 2026-04-10.

https://digitalstate.gov.ua/projects/govtech/diia

Brave1 - thông tin về dự án Brave1. Digital State UA, 2026-01-20.

https://digitalstate.gov.ua/projects/tech/brave1

Fedorov trở thành Bộ trưởng Quốc phòng: Từ Ukraine số đến chiến tranh bằng drone - UNITED24 Media. UNITED24 Media, 2026-01-14.

https://united24media.com/war-in-ukraine/ukraines-new-defense-minister-is-the-mind-behind-the-countrys-digital-transformation-15021

Chuyển đổi số của Ukraine: Đổi mới để tăng sức chống chịu | Harvard Kennedy School. Harvard Kennedy School CID, 2025-03-01.

https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

Ukraine: Đổi mới số và khả năng chống chịu trong thời chiến. Stanford Social Innovation Review, 2023-01-01.

https://ssir.org/articles/entry/wartime_digital_resilience

The IT Army of Ukraine - Phát hành OP 35 | Australian Army Research Centre (AARC). Australian Army Research Centre, 2026-04-22.

https://researchcentre.army.gov.au/library/land-power-forum/it-army-ukraine-release-op-35

Tương lai của drone tại Ukraine: Báo cáo từ Hội nghị DIU-Brave1 Warsaw | Center for Security and Emerging Technology. CSET Georgetown, 2023-10-01.

https://cset.georgetown.edu/article/the-future-of-drones-in-ukraine-a-report-from-the-diu-brave1-warsaw-conference/

· [Mykhailo Fedorov] - Wikipedia, bách khoa toàn thư tự do. Wikipedia zh, 2026-01-14.

https://zh.wikipedia.org/zh-hans/%E7%B1%B3%E5%93%88%E4%BC%8A%E6%B4%9B%C2%B7%E8%B2%BB%E5%A4%9A%E7%BE%85%E5%A4%AB

[Bộ trưởng Chuyển đổi số Ukraine: Ukraine sẽ phát triển
drone chiến đấu không đối không]. Voice of America Chinese, 2022-12-28.

https://www.voachinese.com/a/ukraine-dronzes-20221228/6895952.html

Bộ trưởng quốc phòng 34 tuổi của Ukraine đã cải tổ chiến lược drone: liệu ông có trở thành người ném bóng cứu nguy? Yonhap News, 2026-01-21.

https://www.yna.co.kr/view/AKR20260121165800109

Bốn bước ngoặt trong chiến tranh Nga-Ukraine do thông tin vệ tinh và drone tạo ra. Weekly Chosun, 2026-05-01.

https://weekly.chosun.com/news/articleView.html?idxno=50981

Starlink, biến số mới trong cuộc chiến drone Ukraine-Nga: Ukraine và SpaceX đáp trả bằng cách chặn Nga. Drone Journal, 2026-02-05.

https://www.dronejournal.net/news/articleView.html?idxno=273

Chống lại drone của Nga: Cách hoàn tất xác minh Starlink để vận hành thiết bị đầu cuối tại Ukraine | Tin tức MoD. Ministry of Defence of Ukraine, 2026-02-02.

https://mod.gov.ua/en/news/countering-russian-drones-how-to-complete-starlink-verification-to-operate-terminals-in-ukraine

Drone Line: triển khai một học thuyết tác chiến mới | Tin tức MoD. Ministry of Defence of Ukraine, 2026-04-09.

https://mod.gov.ua/en/news/drone-line-implementing-a-new-warfare-doctrine

UAV dẫn đầu, DELTA vẫn là một thách thức: quân nhân huấn luyện trên ứng dụng Army+ như thế nào | Tin tức MoD. Ministry of Defence of Ukraine, 2026-02-02.

https://mod.gov.ua/en/news/ua-vs-lead-the-way-delta-remains-a-challenge-how-service-members-train-in-the-army-app

Quân nhân sẽ nhận cảnh báo mối đe dọa trên không trong ứng dụng DELTA Mobile | Tin tức MoD. Ministry of Defence of Ukraine, 2026-03-10.

https://mod.gov.ua/en/news/service-members-will-receive-air-threat-alerts-in-the-delta-mobile-app

Mykhailo Fedorov: Ukraine đang nâng cao hiệu quả trên chiến trường và kêu gọi EU tăng cường hỗ trợ quốc phòng | Tin tức Bộ Quốc phòng. Bộ Quốc phòng Ukraine, 2026-03-10.

https://mod.gov.ua/en/news/mykhailo-fedorov-ukraine-is-boosting-battlefield-effectiveness-and-calling-on-the-eu-to-strengthen-defence-support

Estonia chuẩn bị một gói viện trợ mới cho Ukraine, bao gồm drone và năng lực chống drone | Tin tức Bộ Quốc phòng. Bộ Quốc phòng Ukraine, 2026-02-03.

https://mod.gov.ua/en/news/estonia-prepares-a-new-assistance-package-for-ukraine-encompassing-drones-and-counter-drone-capabilities

Ukraine và Đức tăng cường nỗ lực đẩy nhanh việc chuyển giao đạn dược phòng không | Tin tức Bộ Quốc phòng. Bộ Quốc phòng Ukraine, 2026-06-10.

https://mod.gov.ua/en/news/ukraine-and-germany-step-up-efforts-to-accelerate-the-delivery-of-air-defence-munitions

DELTA | Tin tức Bộ Quốc phòng. Bộ Quốc phòng Ukraine, 2024-05-22.

https://mod.gov.ua/en/news/dou-day-2024-conference-ukrainian-developers-presented-delta-combat-system-1

Chương trình "Army of Drones Bonus" mang lại kết quả: gần 820.000 mục tiêu của Nga bị đánh trúng trong năm 2025, Mykhailo Fedorov cho biết | Tin tức MoD. Bộ Quốc phòng Ukraine, 2026-01-26.

https://mod.gov.ua/en/news/army-of-drones-bonus-program-delivers-results-nearly-820-000-russian-targets-hit-in-2025-says-mykhailo-fedorov

Hệ thống tác chiến DELTA của Ukraine vượt qua cuộc kiểm toán của NATO | Tin tức MoD. Bộ Quốc phòng Ukraine, 2024-07-17.

https://mod.gov.ua/en/news/in-ukraine-for-the-first-time-the-cyber-security-of-the-combat-system-was-tested-according-to-nato-standards

Đầu tư vào ngành công nghiệp quốc phòng của Ukraine | Tin tức MoD. Bộ Quốc phòng Ukraine, 2024-11-12.

https://mod.gov.ua/en/news/ministry-of-defense-urges-european-partners-to-invest-in-ukraine-s-defense-industry-including-through-frozen-russian-assets

Bộ Quốc phòng đã ký hợp đồng với số lượng kỷ lục máy bay không người lái đa rotor cho tiền tuyến | Tin tức MoD. Bộ Quốc phòng Ukraine, 2026-03-11.

https://mod.gov.ua/en/news/the-ministry-of-defence-contracted-a-record-number-of-multirotor-drones-for-the-front

Các lữ đoàn chiến đấu đã nhận 500.000 hạng mục, bao gồm drone, hệ thống robot mặt đất và các thiết bị khác, thông qua DOT-Chain Defence | Tin tức MoD. Ministry of Defence of

Ukraine, 2026-03-11.

https://mod.gov.ua/en/news/combat-brigades-received-500-000-items-including-drones-ground-robotic-systems-and-other-equipment-through-dot-chain-defence

Danh sách trắng cho thiết bị đầu cuối Starlink: Cách tìm số KIT và mã định danh UTID để hoàn tất xác minh và sử dụng thiết bị đầu cuối của bạn tại Ukraine | Tin tức MoD. Ministry of Defence of Ukraine, 2026-02-03.

https://mod.gov.ua/en/news/white-list-for-starlink-terminals-how-to-find-the-kit-number-and-utid-identifier-to-complete-verification-and-use-your-terminal-in-ukraine

Brave1 Defense Tech Valley 2026: Ukraine đang định hình một chuẩn mực toàn cầu mới cho các giải pháp quốc phòng | MoD News. Ministry of Defence of Ukraine, 2026-04-09.

https://mod.gov.ua/en/news/brave1-defense-tech-valley-2026-ukraine-is-shaping-a-new-global-standard-for-defense-solutions

Hơn 10 đơn vị quân sự hiện đã được trang bị một tháp pháo Ukraine dùng AI, có khả năng tiêu diệt UAV chỉ bằng một lần nhấn nút | MoD News. Ministry of Defence of Ukraine, 2026-05-09.

https://mod.gov.ua/en/news/over-10-military-units-are-now-equipped-with-a-ukrainian-ai-powered-turret-capable-of-destroying-ua-vs-with-a-single-button-press

«Інформацію потрібно вносити лише один раз»: giáo viên từ vùng Ternopil đã giúp 20 trường học chuyển sang Mriia như thế nào ["Thông tin chỉ cần nhập một lần": một giáo viên từ vùng Ternopil đã giúp 20 trường học chuyển sang Mriia như thế nào]. Ministry of Digital Transformation of Ukraine, 2026-07-10.

https://thedigital.gov.ua/news/education/informatsiiu-potribno-vnosyty-lyshe-odyn-raz-iak-vchytelka-z-ternopilshchyny-dopomohla-20-shkolam-pereyty-na-mriiu

Досліджуємо українське IT: hãy tham gia khảo sát trong khuôn khổ IT Research Ukraine 2026 [Nghiên cứu ngành IT Ukraine: hãy tham gia khảo sát trong khuôn khổ IT Research Ukraine 2026]. Ministry of Digital Transformation of Ukraine, 2026-07-09.

https://thedigital.gov.ua/news/business/doslidzuyemo-ukrayinske-it-doluchaytesia-do-opytuvannia-v-mezakh-it-research-ukraine-2026

Де є енергонезалежний інтернет? Мінцифра та Дія створюють національну мапу xPON-мереж [Ở đâu có internet độc lập về năng lượng? Bộ Chuyển đổi Số và Diia đang xây dựng bản đồ quốc gia về các mạng xPON]. Ministry of Digital Transformation of Ukraine, 2026-07-09.

https://thedigital.gov.ua/news/technologies/de-ye-enerhonezaleznyy-internet-mintsyfra-ta-dia-stvoriuiut-natsionalnu-mapu-xpon-merez

Дія.City в регіонах: де технологічні компанії сплатили найбільше податків у 2025 році [Diia.City tại các vùng: nơi các công ty công nghệ nộp nhiều thuế nhất trong năm 2025]. Ministry of Digital Transformation of Ukraine, 2026-07-08.

https://thedigital.gov.ua/news/regions/diiacity-v-rehionakh-de-tekhnolohichni-kompaniyi-splatyly-naybilshe-podatkiv-u-2025-rotsi

Оцифровуємо українські рукописи: хто переміг в AI-челенджі Handwritten to Data [Số hóa các bản thảo viết tay của Ukraine: ai đã thắng thử thách AI Handwritten to Data]. Ministry of Digital Transformation of Ukraine, 2026-07-08.

https://thedigital.gov.ua/news/shtuchnyy-intelekt/otsyfrovuyemo-ukrayinski-rukopysy-khto-pereminh-v-ai-chelendzi-handwritten-to-data

Від навчання до реального оферу: Мінцифра запустила Кар'єрну студію із симулятором співбесіди на Дія.Освіта [Từ đào tạo đến lời mời làm việc thực tế: Ministry of Digital Transformation đã ra mắt Career Studio với trình mô phỏng phỏng vấn trên Diia.Education]. Ministry of Digital Transformation of Ukraine, 2026-07-08.

https://thedigital.gov.ua/news/education/vid-navchannia-do-realnoho-oferu-mintsyfra-zapustyla-karyernu-studiiu-iz-symuliatorom-spivbesidy-na-diiaosvita

Штучний інтелект у ЦНАПах: яким буде майбутнє державних сервісів [Trí tuệ nhân tạo trong các Trung tâm Dịch vụ Hành chính: tương lai của dịch vụ công sẽ ra sao]. Ministry of Digital Transformation of Ukraine, 2026-07-03.

https://thedigital.gov.ua/news/progress/shtuchnyy-intelekt-u-tsnapakh-iakym-bude-maybutnye-derzavnykh-servisiv

Україна та Естонія створюють AI-рішення для держави майбутнього: на міжнародному хакатоні визначили переможців [Ukraine và Estonia đang xây dựng các giải pháp AI cho nhà nước của tương lai: những người chiến thắng đã được công bố tại một hackathon quốc tế]. Ministry of Digital Transformation of Ukraine, 2026-07-03.

https://thedigital.gov.ua/news/shtuchnyy-intelekt/ukrayina-ta-estoniia-stvoriuiut-ai-rishennia-dlia-derzavy-maybutnyoho-na-miznarodnomu-khakatoni-vyznachyly-peremoztsiv

Italy đã đảm nhận vai trò dẫn dắt Tallinn Mechanism: nước này sẽ phân bổ thêm €1 triệu cho phòng thủ mạng của Ukraine. Ministry of Digital Transformation of Ukraine, 2026-07-01.

https://thedigital.gov.ua/news/technologies/italiia-ocholyla-tallinnskyy-mekhanizm-krayina-vydilyt-shche-eur1-mln-na-kiberzakhyst-ukrayiny

Lập trường của Ministry of Digital Transformation về những tuyên bố mang tính thao túng liên quan đến dự án Diia.City. Ministry of Digital Transformation of Ukraine, 2026-06-30.

https://thedigital.gov.ua/news/business/pozytsiia-mintsyfry-shchodo-manipuliatyvnykh-zaiav-pro-proyekt-diiacity

Цифровізуємо державні сервіси та реєстри швидше, простіше й дешевше: Мінцифра провела форум Дія.Engine [Số hóa các dịch vụ công và cơ sở đăng ký nhanh hơn, đơn giản hơn và rẻ hơn: Ministry of Digital Transformation of Ukraine đã tổ chức diễn đàn Diia.Engine]. Ministry of Digital Transformation of Ukraine, 2026-06-22.

https://thedigital.gov.ua/news/technologies/tsyfrovizuyemo-derzavni-servisy-ta-reyestry-shvydshe-prostishe-y-deshevshe-mintsyfra-provela-forum-diiaengine

Від чинних документів до генерації нових ключів: як і коли відбудеться перехід на новий стандарт е-підпису [Từ các tài liệu hiện có đến việc tạo khóa mới: quá trình chuyển sang tiêu chuẩn chữ ký điện tử mới sẽ diễn ra như thế nào và khi nào]. Ministry of Digital Transformation of Ukraine, 2026-06-25.

https://thedigital.gov.ua/news/technologies/vid-chynnykh-dokumentiv-do-heneratsiyi-novykh-kliuchiv-iak-i-koly-vidbudetsia-perekhid-na-novyy-standart-e-pidpysu

Chuyển đổi Lực lượng Phòng vệ Ukraine: giai đoạn thứ nhất | Mykhailo Fedorov [The transformation of Ukraine's Defence Forces: stage one | Mykhailo Fedorov]. Kênh truyền hình Rada, 2026-06-17.

https://www.youtube.com/watch?v=ytv97owmMn0

FEDOROV. ĐỘC QUYỀN. Chiến tranh sẽ kết thúc như thế nào, lương 300.000 hryvnia trong quân đội, hợp đồng mới và việc giải ngũ [FEDOROV. EXCLUSIVE. How the war will end, 300,000-hryvnia army salaries, new contracts, and demobilisation]. TSN, 2026-06-16.

https://www.youtube.com/watch?v=cTobgzbBMMY

ЦЕ ІНТЕРВ'Ю Федорова НАРОБИЛО такого ГАЛАСУ! На нас чекають капітальні ЗМІНИ в ЗСУ. Ось що готується [CUỘC PHỎNG VẤN NÀY với Fedorov đã gây ra một làn sóng ồn ào như vậy! Những THAY ĐỔI sâu rộng đang chờ Lực lượng Vũ trang. Đây là những gì đang được chuẩn bị]. Ми - Україна, 2026-06-18.

https://www.youtube.com/watch?v=3RjW0qVk1S4

Федоров сказав КОЛИ БУДЕ ДЕМОБІЛІЗАЦІЯ! Ексклюзивно про ТРАНСФОРМАЦІЮ Сил оборони [Fedorov đã nói KHI NÀO SẼ CÓ GIẢI NGŨ! Nội dung độc quyền về SỰ CHUYỂN ĐỔI của Lực lượng Phòng vệ]. УНІАН TV, 2026-06-17.

https://www.youtube.com/watch?v=fXtp18GwIjg

TOÀN BỘ CHÍNH PHỦ TỪ CHỨC! Chỉ có MỘT ĐIỂM SÁNG. Fedorov ĐÃ ĐI NGƯỢC LẠI SYRSKYI. Cái bẫy của Bankova [TOÀN BỘ CHÍNH PHỦ TỪ CHỨC! Chỉ có MỘT ĐIỂM SÁNG. Fedorov đã ĐI NGƯỢC LẠI SYRSKYI. Cái bẫy của Bankova]. Фабрика новин, 2026-07-10.

https://www.youtube.com/watch?v=kE4-WiKxx2E

Hành động tiếp theo như thế nào? Mykhailo Fedorov | Business Breakfast với Volodymyr Fedorin [Hành động tiếp theo như thế nào? Mykhailo Fedorov | Business Breakfast với Volodymyr Fedorin]. Forbes Ukraine, 2024-02-07.

https://www.youtube.com/watch?v=1eSQGaYyLS0

Михайло Федоров: «Дія»: bầu cử và điều tra dân số, chiến tranh mạng, thư từ với Musk | Phỏng vấn [Mykhailo Fedorov: "Diia": bầu cử và điều tra dân số, chiến tranh mạng, thư từ với Musk | Phỏng vấn]. Радіо Свобода, 2023-02-04.

https://www.youtube.com/watch?v=AT24xJqQ-IA

Інновації, які змінюють хід війни: Mykhailo Fedorov nói về drone, tác chiến điện tử và Brave1 | Podcast Slon [Những đổi mới đang thay đổi cục diện chiến tranh: Mykhailo Fedorov nói về drone, tác chiến điện tử và Brave1 | Podcast The Slon]. Дія, 2024-01-12.

https://www.youtube.com/watch?v=63aDfQlslKU

ЦІЄЇ МИТІ! FEDOROV ĐÃ ĐÈ BẸP NGƯỜI NGA! ĐÒN ĐÁNH CUỐI CÙNG CỦA LỰC LƯỢNG VŨ TRANG UKRAINE: NGA ĐANG BỐC CHÁY! PUTIN ĐÃ CỨNG HỌNG! [KHOẢNH KHẮC NÀY! FEDOROV ĐÃ ĐÈ BẸP NGƯỜI NGA! ĐÒN ĐÁNH CUỐI CÙNG CỦA LỰC LƯỢNG VŨ TRANG: NGA ĐANG BỐC CHÁY! PUTIN ĐÃ CỨNG HỌNG!]. СПЕЦКОР | Новини 2+2, 2026-07-12.

https://www.youtube.com/watch?v=U4OddMn3eQw

Nội các chiến tranh mới của Ukraine được giải thích: Điều gì thay đổi từ bây giờ? (Budanov, Fedorov, khủng hoảng năng lượng). KI Insights, 2026-01-28.

https://www.youtube.com/watch?v=5z6NhcHIf5Q

Bộ trưởng Quốc phòng Ukraine: Crimea trở thành một hòn đảo | Cách mạng quân đội | Ukraine thay đổi chiến tranh như thế nào. PEICHEV, 2026-06-17.

https://www.youtube.com/watch?v=oN3zPUlnFWc

СТЕРНЕНКО | УДАРИ ПО РОСІЇ | ПРО "СКЕЛЮ" | РАДНИК У ФЕДОРОВА | Removska [STERNENKO | CÁC CUỘC TẤN CÔNG VÀO NGA | VỀ "SKELIA" | CỐ VẤN CỦA FEDOROV | Removska]. Суспільне Новини, 2026-07-11.

https://www.youtube.com/watch?v=IfjIS883a7g

ФЕДОРОВ: QUAN HỆ VỚI SYRSKYI / TIN ĐỒN TỪ CHỨC / CÁC NHÓM THAM NHŨNG TRONG LĨNH VỰC QUỐC PHÒNG [FEDOROV: RELATIONS WITH SYRSKYI / RESIGNATION RUMOURS / CORRUPT CLANS IN THE DEFENCE SECTOR]. PRESSING, 2026-06-17.

https://www.youtube.com/watch?v=EWuI8WYOfF8

CUỘC PHỎNG VẤN DÀI VỚI MYKHAILO FEDOROV | Bộ Quốc phòng Ukraine, drone, công nghệ và tương lai [A LONG INTERVIEW WITH MYKHAILO FEDOROV | The Ministry of Defence of Ukraine, drones, technology, and the future]. УП UKRAINIAN TRUTH, 2026-06-19.

https://www.youtube.com/watch?v=p-Js4_cbkpE

Після ТЕРОРУ у Києві ФЕДОРОВ озвучив ГАРНІ НОВИНИ! Ця ЗВІСТКА СКОЛИХНУЛА СВІТ. Цього Путін І БОЯВСЯ [Sau vụ KHỦNG BỐ ở Kyiv, FEDOROV đã công bố TIN TỐT LÀNH! BẢN TIN này đã LÀM RUNG CHUYỂN THẾ GIỚI. Đây chính là điều Putin LO SỢ]. 24 Канал онлайн, 2026-07-03.

https://www.youtube.com/watch?v=Gvm4NZ35cHM

ТЕРМІНОВА ЗВІСТКА від ФЕДОРОВА! Ось, що ОГОЛОСИЛИ українцям. СТЕРНЕНКО ПОЯСНИВ, що чекати [TIN KHẨN từ FEDOROV! Đây là điều đã được CÔNG BỐ với người Ukraine. STERNENKO GIẢI THÍCH điều cần chờ đợi]. 24 Канал, 2026-03-11.

https://www.youtube.com/watch?v=zVIlLiUj6sQ

ФЕДОРОВ вразив зверненням до українців! Такого успіху ще не було. АРАБСЬКИЙ світ відповів КИЄВУ [FEDOROV gây chấn động với bài phát biểu gửi người Ukraina! Chưa từng có thành công nào như thế này. Thế giới Ả Rập đã trả lời KYIV]. 24 Канал, 2026-04-02.

https://www.youtube.com/watch?v=vP1KN2DstD4

ЩОЙНО! НАД УКРАЇНОЮ ЗАКРИЛИ НЕБО! ФЕДОРОВ ЦЕ ЗРОБИВ: РІШЕННЯ ЯКЕ ПЕРЕВЕРНУЛО ВСЕ! | ПРЯМО ЗАРАЗ [TIN VỪA ĐẾN! BẦU TRỜI TRÊN UKRAINA ĐÃ BỊ ĐÓNG! FEDOROV ĐÃ LÀM ĐIỀU ĐÓ: QUYẾT ĐỊNH LÀM THAY ĐỔI TẤT CẢ! | NGAY LÚC NÀY]. УКРАЇНА СЬОГОДНІ, 2026-02-27.

https://www.youtube.com/watch?v=0UYBFYulNzk

Điều Fedorov dự định thực hiện gây ấn tượng mạnh. Thay đổi toàn diện hệ thống huy động thông qua các trung tâm tuyển quân | Maksym Kostetskyi [Những gì Fedorov đã lên kế hoạch thật đáng chú ý. Một cuộc cải tổ toàn diện hệ thống huy động thông qua các trung tâm tuyển quân | Maksym Kostetskyi]. Radio NV, 2026-04-24.

https://www.youtube.com/watch?v=MQRiiiWjRS0

Fedorov như tấm gương phản chiếu Zelensky. Vì sao các quân nhân bắt đầu bị thẩm vấn. Họ MUỐN bầu cử qua Diia [Fedorov như tấm gương phản chiếu Zelensky. Vì sao các quân nhân bắt

đầu bị thẩm vấn. Họ MUỐN bầu cử thông qua Diia]. Dana Yarova, 2026-02-16.

https://www.youtube.com/watch?v=OQcOmxjz3S8

ФЕДОРОВ: BRAVE1 - НАЙБІЛЬШИЙ АНГЕЛЬСЬКИЙ ІНВЕСТОР УКРАЇНИ | ДІПСТРАЙКИ, ЗЕНІТНІ ДРОНИ, МАШИННИЙ ЗІР [FEDOROV: BRAVE1 là nhà đầu tư thiên thần lớn nhất của Ukraine | Các cuộc tấn công tầm sâu, drone phòng không, thị giác máy]. Army TV - Ukrainian military channel, 2025-09-22.

https://www.youtube.com/watch?v=ePBwCKgrdrg

Pistorius y Fédorov a 30 km del frente: Alemania entra en Brave1 y el fracaso de los planes de Rusia [Pistorius và Fedorov cách tiền tuyến 30 km: Đức tham gia Brave1 và sự thất bại trong các kế hoạch của Nga]. UATV Español, 2026-06-23.

https://www.youtube.com/watch?v=zAS7t-oO5HE

100 ngày của Fedorov / Mái vòm chống drone / Hỗn loạn trong phòng không tầm ngắn - YELIZAROV | Ukrainska Pravda. Phỏng vấn [100 days of Fedorov / The counter-drone dome / Chaos in short-range air defence - YELIZAROV | Ukrainska Pravda. Interview]. Ukrainska Pravda, 2026-04-30.

https://www.youtube.com/watch?v=nR3SYLP1CfE

PISTORIUS VÀ FEDOROV GẦN TIỀN TUYẾN: cuộc trao đổi về BRAVE1, MID-STRIKE và NHỮNG THAY ĐỔI TRONG CHIẾN TRANH HIỆN ĐẠI [PISTORIUS AND FEDOROV NEAR THE FRONT: a conversation on BRAVE1, MID-STRIKES, and the CHANGES IN MODERN WAR]. UATV po polsku, 2026-06-07.

https://www.youtube.com/watch?v=BL4d96Uw3O0

Oleksandr Bornyakov nói về tương lai của Bộ Chuyển đổi Số, xuất khẩu vũ khí, Brave1, sản xuất chip và LLM của Ukraine [Oleksandr Bornyakov on the future of the Ministry of Digital Transformation, arms exports, Brave1, chip manufacturing, and a Ukrainian LLM]. UT-2, 2026-01-27.

https://www.youtube.com/watch?v=BI0ZWuLFXQM

Support This AI Library Book

If this book was useful, you can support future translations, public editions, and open AI knowledge projects through PayPal.

PayPal

https://paypal.me/kimkjj

Scan the QR code or open the link above.