

## Bài học từ Ukraine Phần 2. Hết

### Tác chiến điện tử và cuộc chiến gây nhiễu

**Nguồn:** Shashank Joshi, [The latest in the battle of jamming with electronic beams](#), *The Economist*, 03/7/2023

**Biên dịch:** Nguyễn Thế Phương

26/7/2023



**Xem thêm:** [Phần 1](#)

Gây nhiễu đang là biện pháp hữu để hiệu loại bỏ drone và tên lửa khỏi bầu trời.

Khi các pháo thủ Ukraine bắt đầu sử dụng các quả đạn pháo có độ chính xác cao Excalibur vào khoảng thời gian đầu cuộc chiến, họ thật sự rất hài lòng, và có phần tự đắc. Với các loại đạn pháo thông thường, các pháo thủ phải bắn nhiều loạt đạn vào mục tiêu để tiêu diệt chúng, ngay cả khi họ biết chính xác họ đang nhắm vào đâu. Excalibur, được dẫn đường bằng GPS, dường như đã trở thành một “viên đạn bạc”: một phát bắn, và một mục tiêu bị tiêu diệt. Thế nhưng, vào tháng 3 năm 2023 có thứ gì đó đã thay đổi. Các quả đạn Excalibur chỉ đơn giản là rơi từ trên trời xuống theo đúng nghĩa đen, hay thất bại trong việc tiêu diệt mục tiêu. Và điều này xảy ra không chỉ một lần: hàng tuần trôi qua mà không có mục tiêu nào bị tiêu diệt thành công. Đây là một lời nhắc nhở đáng lo ngại về tác động sâu sắc của tác chiến điện tử (electronic warfare) tới cuộc chiến tại Ukraine.

Nếu chiến tranh hiện đại dựa trên 3 trụ cột chính – các loại cảm biến ngày càng tân tiến để phát hiện mục tiêu, các loại đạn được ngày càng chính xác để tấn công mục tiêu, và các mạng

lưới kết nối hai thành tố đó lại với nhau – thì tác chiến điện tử đe dọa làm sút mẻ cả 3 trụ cột nói trên. Các quả đạn Excalibur rơi rụng như ruồi là do Nga đã sử dụng các thiết bị gây nhiễu làm gián đoạn tín hiệu GPS hướng chúng tới mục tiêu, hay nhiều khả năng hơn, là gây nhiễu đầu nổ ra-đa vốn giúp các quả đạn xác định thời điểm phát nổ chính xác. Excalibur không phải là loại vũ khí duy nhất bị “gây mù” theo kiểu đó.

Các tài liệu rò rỉ từ Lầu Năm Góc kể từ mùa xuân cho thấy 4 trong tổng số 9 đợt không kích của Ukraine sử dụng bom JDAM-ER do Mỹ cung cấp có thể đã trượt mục tiêu do các hoạt động gây nhiễu GPS từ phía Nga. “Các khí tài gây nhiễu của Nga thuộc dạng ưu tiên cao”, theo một slide báo cáo, “và chúng tôi tiếp tục đề xuất rằng các khí tài đó phải bị ngăn chặn/tiêu diệt...càng nhiều càng tốt”. GMLRS, các quả đạn rốc két dẫn đường chính xác được sử dụng bởi HIMARS, bắn trượt mục tiêu càng ngày càng nhiều, hoặc là chúng đã không đạt được hiệu quả như mong muốn. Bầu trời ở Kyiv và Moscow dày đặc các loại sóng gây nhiễu khi cả hai bên đều muốn vô hiệu hoá drone và tên lửa của nhau.

Phương thức tác chiến điện tử như trên là không mới. Nó có khả năng đã bắt đầu vào năm 1904 trong Chiến tranh Nga-Nhật. Mặc dù bom đạn thời điểm đó là bom đạn “ngu” – công nghệ đầu nổ ra-đa cận đích phải 40 năm nữa mới ra đời, trong khi các vệ tinh GPS là hơn 70 năm – thì kỷ nguyên của radio đã tới. Một nhân viên vận hành đài radio người Nga ở Port Arthur (nay là Lữ Thuận Khẩu, Trung Quốc – ND) đã táo bạo “nhấn chìm” toàn bộ đường truyền tín hiệu từ một tàu chiến Nhật Bản gần đó vốn đang làm nhiệm vụ dẫn bắn cho pháo hạm. Trong cuộc chiến sóng tín hiệu (battle of the beams) ở Thế chiến thứ hai, nước Anh đã gây nhiễu và đánh lừa tín hiệu radio được sử dụng bởi các máy bay ném bom Đức đang trên đường tới mục tiêu. Và khi mà sức mạnh không quân ngày càng trở nên quan trọng trong Chiến tranh Lạnh, phát hiện và gây nhiễu tín hiệu ra-đa phòng không trở thành một nhiệm vụ tối quan trọng.

Nước Nga từ lâu đã được đánh giá là vượt trội về mặt này. Moscow đầu tư mạnh mẽ vào các khí tài tác chiến điện tử từ một thập kỷ trước, cũng như thử nghiệm các khí tài này tại Ukraine năm 2014 và sau đó là ở Syria vào năm 2015, vốn thường gây ra một số gián đoạn cho các hãng hàng không dân dụng. Tuy nhiên, cuộc xâm lược của Nga vào Ukraine lại cho thấy một

bức tranh hỗn hợp. Tác chiến điện tử Nga có “hiệu quả cao” ở một số mặt, theo kết luận của RUSI. Các máy bay chiến đấu của Ukraine ban đầu nhận thấy rằng hệ thống thông tin liên lạc, dẫn đường cũng như ra-đa của họ bị gián đoạn, và trong một số trường hợp là hoàn toàn bị vô hiệu hoá. Việc các quả đạn pháo Excalibur bị “làm mù” khiến cho các quan chức phương Tây lo ngại. Thế nhưng, năng lực trên đất liền cũng như trên biển của Nga còn “nhiều hạn chế”, theo lập luận của Thomas Withington, một chuyên gia phân tích về tác chiến điện tử. “Phân tích trước chiến tranh của chúng tôi về năng lực tác chiến điện tử Nga là không mấy lạc quan”, theo Edward Stringer, một trung tướng không quân đã về hưu của Không lực Hoàng gia Anh. “Tác chiến điện tử Nga hoàn toàn có thể bị đánh bại”.

Tuy nhiên, một binh sĩ điều khiển drone trên chiến trường có thể không hoàn toàn đồng ý với nhận định trên. Ukraine thi thoảng đã phải hứng chịu thiệt hại lên tới 10.000 drone trong một tháng. Một nửa số drone bị hạ là do các cuộc tấn công điện tử, theo Andriy (không phải tên thật), một sĩ quan cao cấp của cơ quan tham mưu Ukraine. Gây nhiễu thông thường sẽ ngăn chặn tín hiệu giúp điều khiển drone từ xa, hay ngăn chặn đường truyền thông tin liên lạc được sử dụng để truyền dữ liệu. Người điều khiển drone có thể khắc phục bằng cách cho drone di chuyển theo một đường bay được quy định trước, và tải dữ liệu xuống khi drone quay trở về, thế nhưng làm như thế sẽ khiến cho việc xác định mục tiêu bị kéo dài ra vài giờ đồng hồ. Và bản thân biện pháp trên không giải quyết được vấn đề cốt lõi: rằng hầu hết các drone bị vô hiệu hoá khi tín hiệu GPS bị ngăn chặn, và khiến cho chúng bay đi mất trong tình trạng không người điều khiển.

Điều này tạo ra một sự đánh đổi tương đối lớn cho phe phòng thủ. Các drone quân sự (và tên lửa) được lắp đặt các bộ thu tín hiệu đặc biệt có thể thu nhận tín hiệu “M-code” từ các vệ tinh GPS của Mỹ. Các tín hiệu đó có mức năng lượng cao hơn nhiều so với GPS dân sự và được mã hoá, khiến cho chúng dễ bị phát hiện nhưng lại khó bị gây nhiễu – mà theo Dana Goward, chủ tịch của Quỹ Resilient Navigation and Timing, một tổ chức phi chính phủ ở Virginia – là khó hơn gấp 8 lần. Thế nhưng các bộ thu tín hiệu M-code bị áp đặt các biện pháp hạn chế xuất khẩu và có giá mắc hơn thông thường. Nếu tiến hành các biện pháp bảo vệ điện tử trên drone

sẽ tốn thêm kinh phí và làm cho drone nặng hơn. Hạm đội drone của Ukraine hiện tại đang rẻ tới mức có thể dễ dàng chấp nhận tiêu hao.

Điều đó đang thay đổi, mặc dù với tốc độ chậm. Các quan chức Ukraine đang hy vọng có thể dần thay thế các drone thương mại DJI của Trung Quốc, loại drone đang được cả hai bên cùng sử dụng trên tiền tuyến, bằng các thiết bị chuyên nghiệp hơn. “Một trong những bài học rút ra được từ Ukraine chính là việc sở hữu các kết nối radio không mã hoá không còn là một lựa chọn nữa”, theo Withington. “Nếu bạn là NATO, bạn cần phải mã hoá mọi thứ”. Thậm chí khi đó, M-code chỉ có thể đem lại một số lợi ích “không mấy quan trọng”, Goward đưa ra cảnh báo, bởi vì công nghệ đó đã có tuổi đời hai thập kỷ và tín hiệu GPS về bản chất đã là một loại tín hiệu yếu.

Yếu không có nghĩa là không sử dụng được. Các đội quân phương Tây từ lâu đã lo ngại rằng sự chớp nhoáng trong sử dụng tác chiến điện tử từ Nga có thể giúp nước này chống lại lợi thế về công nghệ của họ. “Tác chiến điện tử là tác nhân lớn giúp san bằng khoảng cách”, thiếu tướng Charles Collins, phó tổng tham mưu trưởng lục quân Anh, đã viết như vậy trong một báo cáo gần đây. “Bằng cách triệt tiêu các yếu tố kết nối, nó kéo quân đội lùi về thế kỷ 20”. Tuy nhiên, điều đó chưa được chứng minh là đúng tại Ukraine.

Trên thực tế, gây nhiễu là không hoàn hảo và gián đoạn. Một nguyên nhân là do các hệ thống tác chiến điện tử là của hiếm. Nga buộc phải giữ một vài hệ thống ở hậu phương để bảo vệ các thành phố và căn cứ quân sự. Nguyên nhân khác là do là cái giá phải trả khi triển khai các hệ thống như vậy. Khí tài gây nhiễu lớn thường phát ra tín hiệu mạnh, khiến chúng trở thành các mục tiêu dễ bị phát hiện. Nga đã phải tái triển khai các thiết bị tốt nhất của mình lùi sâu ở hậu phương, theo một quan chức. Và điều này tạo ra các lỗ hổng chờ bị khai thác. Mỹ đang cung cấp cho Ukraine các bản đồ liên quan tới hoạt động điện tử – về căn bản là vị trí của các hoạt động gây nhiễu cũng như tần suất sử dụng – 32 lần một ngày, theo T.J. Holland từ Quân đoàn 18 của Mỹ. Chính sách này mang lại lợi ích lớn cho các binh sĩ điều khiển drone của Ukraine.

### **Gây nhiễu chính các khí tài gây nhiễu**

Kết luận rằng tác chiến điện tử đã cắt đứt hoàn toàn thông tin liên lạc là không đúng. Nga đã thất bại trong việc vô hiệu hoá các thiết bị Starlink vốn giúp quân đội Ukraine có thể tiếp cận

hầu như không hạn chế internet qua vệ tinh. Một nguyên nhân là do tín hiệu đường truyền Starlink là cực kỳ hẹp – bạn phải tiếp cận 100-200 mét mới phát hiện ra nó, theo Andriy. Các khí tài tác chiến điện tử của Nga dường như cũng không thể gây nhiễu tần số radio của Starlink hay các thiết bị radio chiến thuật SINCGARS mà Mỹ cung cấp cho Ukraine, theo Withington.

Nếu như tác chiến điện tử Nga thường xuyên gây thất vọng, thì trong nhiều trường hợp chúng lại trở nên mạnh mẽ quá mức cần thiết. Một báo cáo của Justin Bronk và đồng nghiệp tại RUSI mô tả về một sự kiện “huynh đệ tương tàn nghiêm trọng” liên quan tới tác chiến điện tử. Khi cuộc xâm lược đã diễn ra được 2 ngày, Nga đã phải kéo giảm quy mô của chiến dịch gây nhiễu trên bộ bởi hành động này đã ảnh hưởng tiêu cực tới thông tin liên lạc của chính quân đội Nga. Đây là một lý do trả lời cho câu hỏi tại sao các ra-đa phòng không của Ukraine có thể được tái khởi động, giúp bắn rơi một số lượng lớn máy bay chiến đấu Nga vào tháng 3 năm 2022. Thêm vào đó, các máy bay phản lực Nga bay theo cặp cũng đã nhận ra rằng thiết bị tác chiến điện tử gắn trên một máy bay sẽ ảnh hưởng tới ra-đa của máy bay còn lại. Kết quả là, họ phải chọn giữa việc gây nhiễu các tên lửa đang bay tới, hoặc là có một ra-đa có thể hoạt động bình thường.

Có nhiều cách khác nữa để đánh bại tác chiến điện tử. Drone vốn đã bị gây nhiễu GPS có thể hoạt động dựa trên phương thức so sánh địa hình (terrain matching): so sánh hình ảnh địa hình bên dưới với một bản đồ đã được tích hợp sẵn. Kỹ thuật này ra đời từ những năm 1950 và đã được sử dụng bởi nhiều loại tên lửa hành trình, ví dụ như Tomahawk của Mỹ. Thế nhưng các thuật toán hiện đại cùng sức mạnh vi tính đã cho phép so sánh địa hình được thực hiện với độ chính xác cao hơn, giá rẻ hơn, và trên một con chip nhỏ hơn.

GPS cũng có thể được hỗ trợ bởi tín hiệu từ các vệ tinh liên lạc ở quỹ đạo thấp (ví dụ như Starlink), các cơ sở truyền phát tín hiệu mặt đất (như hệ thống Loran của Nga) hay thậm chí là định vị từ trường, theo Goward. Và khi mà vũ khí đang ngày càng tiến hoá trở thành những chiếc máy tính biết phát nổ, ranh giới giữa tác chiến điện tử và tấn công mạng đang mờ đi. Andriy, vị quan chức Ukraine, tiết lộ rằng Ukraine thường xuyên chen các đoạn mã độc vào các drone của Nga ngay cả khi chúng đang ở trên không.

Tác chiến điện tử là một trò chơi mèo vờn chuột. Cả Nga và Ukraine đều đang muốn đạt được “thống trị điện tử” (electromagnetic supremacy), theo Withington, nhưng không nước nào có thể đạt được mục tiêu đó. “Kiểm soát chiến trường sẽ như cơn thủy triều lên xuống”. Các khí tài gây nhiễu sẽ tìm được cách phát huy tác dụng; bên phòng thủ cuối cùng cũng sẽ tìm được cách lấp lỗ hổng. Theo các tài liệu rò rỉ, người Mỹ đang giúp giải quyết vấn đề xảy ra với JDAM-ER bằng cách đảm bảo rằng chúng nhận được đầy đủ tín hiệu GPS trước khi rời khỏi máy bay. Excalibur lại đang một lần nữa đánh phá mục tiêu, theo một quan chức phương Tây. Andriy nói rằng “trong tác chiến điện tử, mọi thứ diễn ra rất nhanh”. Cuộc chiến tuy vậy vẫn phải tiếp diễn. “Trong cuộc chiến này, chúng tôi nhận ra rằng nếu như không thống trị môi trường điện tử, thì không thể hoạt động hiệu quả trong những môi trường tác chiến khác”.

<https://nghienccuquocte.org/2023/07/26>