SÂU MÁY TÍNH STUXNET VÀ TƯƠNG LAI CHIẾN TRANH MẠNG

Nguồn: James P. Farwell & Rafal Rohozinski (2011). "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy*, Vol. 53, No. 1, pp. 23-40.

Biên dịch và Hiệu đính: Lê Hồng Hiệp

Phát hiện vào tháng 6/2010 rằng một sâu máy tính có tên gọi "Stuxnet" đã tấn công một cơ sở hạt nhân của Iran tại Natanz cho thấy rằng đối với chiến tranh mạng tương lai chính là lúc này. Stuxnet dường như đã nhiễm vào hơn 60.000 máy tính, quá nửa trong số đó là ở Iran; các nước khác cũng bị ảnh hưởng bao gồm Ấn Độ, Indonesia, Trung Quốc, Azerbaijan, Hàn Quốc, Malaysia, Mỹ, Anh, Australia, Phần Lan và Đức. Virus tiếp tục lan rộng và nhiễm vào các hệ thống máy tính thông qua internet, mặc dù sức phá hủy của nó giờ đây đã bị hạn chế bởi sự có mặt của các biện pháp khắc phục hiệu quả và cơ chế tự hủy của sâu được xác định vào ngày 24/6/2012.[1]

[1] Symantec nó việc phát hiện diễn ra vào tháng 7/2010, các tin tức báo chí lại cho là vào tháng 6. Báo cáo của *Computer World* cho rằng các nhà nghiên cứu tại hãng bảo mật Belarus là VirusBlokAda đã tìm thấy nó vào tháng 7 trên các máy tính ở Iran. Xem Robert McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems', *Computerworld,* 14 September 2010, http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems; Mark Clayton, 'Stuxnet Malware is "Weapon" Out to Destroy … Iran's Bushehr Nuclear Plant?', *Christian Science Monitor*, 21 September 2010; Mark Clayton, 'How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant', *Christian Science Monitor*, 16 November 2010; John Makoff, 'A Silent Attack, but not a Subtle One', *New York Times*, 26 September 2010. Symantec thiết kế ngược Stuxnet và đưa ra một báo cáo kỹ thuật chi tiết về hoạt động của Stuxnet: Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier', *Symantec Security Response*, Version 1.3, November 2010. Trong thuật ngữ mạng, sâu (worm) là một chương trình hoặc mã độc hại được chèn vào các hệ thống máy tính mà không được sự cho phép của người dùng hay người dùng không hay biết. Chúng lây lan một

Chuyên gia người Đức Ralph Lagner đã miêu tả Stuxnet như một tên lửa mạng cấp độ quân sự được sử dụng để tiến hành một "cuộc tấn công mạng toàn diện chống lại chương trình hạt nhân của Iran".[2] Liam O Murchu, Giám đốc bộ phận Phản ứng An ninh của Symantec, công ty đã thiết kế ngược (reverse-engineer – tức thiết kế dựa vào sản phẩm đã có sẵn – ND) con sâu máy tính và đưa ra một báo cáo chi tiết về cách vận hành của nó, đã tuyên bố rằng "Chúng ta chắc chắn chưa bao giờ nhìn thấy thứ nào như thế này trước đây."[3] Tạp chí *Computer World* gọi đó là "một trong những mẫu phần mềm tinh vi và bất thường nhất từng được tạo ra".[4]

Những tuyên bố này thật thuyết phục. Stuxnet có các đặc tính kỹ thuật mạnh. Tuy nhiên quan trọng hơn là bối cảnh chính trị và chiến lược mà ở đó các mối đe dọa an ninh mạng mới đang xuất hiện, cũng như các tác động mà sâu đã tạo ra liên quan tới bối cảnh này. Có lẽ đáng ngạc nhiên hơn cả là sự hội tụ giữa tội phạm mạng và các hành động của nhà nước. Các nhà nước đang tận dụng công nghệ vốn được thúc đẩy bởi tội phạm mạng, và có lẽ thuê ngoài (outsource) các bên thứ ba không thể quy trách nhiệm thực hiện các cuộc tấn cộng mạng, trong đó bao gồm cả các tổ chức tội phạm.

Sâu máy tính trong vai trò vũ khí

Stuxnet là một chương trình máy tính tinh vi được thiết kế để xâm nhập và giành quyền kiểm soát đối với các hệ thống từ xa theo một cách thức bán tự chủ. Nó đại diện cho một thế hệ mới các phần mềm độc hại dạng sử dụng một lần ("fire-and-forget" malwares). Các đối tượng mà Stuxnet nhắm tới đều được cách ly (air-gapped), nghĩa là chúng không kết nối với mạng internet công cộng và sự xâm nhập đòi hỏi phải sử dụng các thiết bị trung gian ví dụ như USB để giành quyền tiếp cận và thiết lập kiểm soát. Khai thác bốn "lỗ hổng bảo mật ngày số không" (zero-day vulnerabilities – tức các lỗ hổng chưa từng được biết tới, vì vậy không có thời gian để phát triển và phân phối các miếng vá), Stuxnet đã sử dụng các password mặc định của Siemens để truy cập vào các hệ điều hành Windows vốn

---

cách tự động từ máy này sang máy khác và có thể tự nhân lên hàng trăm nghìn lần. Xem 'Worms', OnlineCyberSafety, http://www.bsacybersafety.com/threat/worms.cfm.

[2] Clayton, 'Stuxnet Malware is "Weapon"'. Langner đã viết rất nhiều về Stuxnet trên blog của mình tại địa chỉ http://www.langner.com/en/. Đặc biệt xem thêm Ralph Langner, 'The Big Picture', 19 November2010, http://www.langner.com/en/2010/11/19/thebig-picture/.

[3] McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems'.

[4] Như trên.

được sử dụng để vận hành các chương trình WinCC và PCS 7.[5] Đây là các chương trình Điều kiển logic lập trình được (PLC) vốn được sử dụng để quản lý các nhà máy. Sự tài tình của sâu nằm ở chỗ nó có thể tấn công và lập trình lại một máy tính mục tiêu.[6]

Đầu tiên Stuxnet sẽ truy tìm các thiết bị kiểm soát biến tần (frequency-converter drives) được chế tạo bởi hãng Fararo Paya của Iran và Vacon của Phần Lan. Các thiết bị này được điều khiển bởi các câu lệnh máy tính PLC vốn kiểm soát tốc độ của motor bằng cách điều tiết lượng điện cấp cho motor. Những thiết bị này được đặt ở tốc độ rất cao vốn cần để giúp cho các máy ly tâm tách và tổng hợp các đồng vị uranium-235 phục vụ cho các lò phản ứng nước nhẹ, và nếu được làm giàu cao hơn, có thể sử dụng làm nguyên liệu phân hạch trong các vũ khí nguyên tử.[7]

Stuxnet sau đó thay đổi tần số dòng điện vận hành các máy ly tâm, khiến chúng thay đổi tốc độ lúc nhanh lúc chậm theo các quãng thời gian khác với thiết kế của máy. Nhà nghiên cứu của Symantec Eric Chien miêu tả quá trình đó như sau: "Stuxnet thay đổi tần số dòng điện phát ra và vì vậy thay đổi tốc độ động cơ trong các quãng ngắn nhưng kéo dài hàng tháng trời. Can thiệp vào tốc độ động cơ sẽ phá hoại sự hoạt động bình thường của quy trình quản lý công nghiệp."[8] Tinh vi hơn, sâu còn chứa một rootkit (phần mềm ẩn) giúp che dấu các câu lệnh được download từ các hệ thống của Siemens.

Một số bài báo đã nhầm lẫn khi cho rằng lò phản ứng nước nhẹ của Iran đặt tại Bushehr cũng là một mục tiêu. Iran khẳng định rằng Stuxnet đã xâm nhập vào các máy tính cá nhân nhưng phủ nhận việc sâu tạo ra các thiệt hại nghiêm trọng.[9] Nhưng Bushehr khó có thể là mục tiêu vì plutonium được sản xuất bởi các lò phản ứng nước nhẹ như vậy không phù hợp với mục đích chế tạo vũ khí. Mục tiêu khả dĩ hơn chính là chương trình làm giàu uranium của Iran. Mặc dù phần lớn 4-5.000 máy ly tâm hoạt động cho tới bây giờ tại các cơ sở làm giàu nhiên liệu quy mô công nghiệp hay thử nghiệm tại Natanz đã sản xuất chỉ loại uranium độ giàu thấp, nhưng chính các máy ly tâm này cũng có thể được sử dụng để chế ra loại uranium độ giàu

[5] Xem G. Garza, 'Stuxnet Malware Used 4 Zero-day Exploits', 7-windows.com, 14 September 2010, http://www.7-windows.com/stuxnetmalware-used-4-zero-day-exploits/.
[6] McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems'.
[7] Clayton, 'Stuxnet Malware is "Weapon"'; William J. Broad and David E. Sanger, 'Worm was Perfect for Sabotaging Centrifuges', *New York Times,* 18 November 2010.
[8] Eric Chien, 'Stuxnet: A Breakthrough', Symantec.com, 12 November 2010, http://www.symantec.com/connect/blogs/stuxnet-breakthrough.
[9] David E. Sanger, John Markoff and William Young, 'Iran Fights Malware Attacking Computers', *New York Times*, 25 September 2010; William Yong, 'Iran Denies Malware Connection to Nuclear Delay', *New York Times*, 5 October 2010; William Yong, 'Iran Says it Arrested Computer Worm Suspects', *New York Times*, 2 October 2010.

cao có thể sử dụng làm vũ khí. Hoặc trong một kịch bản khả dĩ hơn nữa, người ta sợ rằng Iran có thể đang vận hành các cơ sở thiết bị ly tâm bí mật để chế tạo uranium độ giàu cao. Điều cốt yếu của Stuxnet là nó có thể tấn công cả những máy ly tâm được biết tới lẫn chưa được biết tới.

Các dạng thức chiến tranh mạng đang nổi lên

Để hiểu được tầm quan trọng chiến lược của Stuxnet cần phải làm rõ những ngộ nhận về nó. Hãy quên đi những thêu dệt trên báo chí. Stuxnet ít phức tạp và tiên tiến hơn nhiều so với miêu tả của báo giới. Một số đặc tính kỹ thuật của nó, bao gồm cả việc sử dụng mạng lưới kiểm soát và điều khiển dựa trên DNS, khiến cho nó dễ bị phát hiện hơn so với các malware mà giới tội phạm sử dụng. Các khả năng và thủ thuật của Stuxnet, bao gồm việc khai thác các lỗ hổng bảo mật ngày số không, khiến nó giống với một biện pháp kết hợp các thủ thuật, các đoạn mã và thực tiễn tốt đúc rút từ giới tội phạm mạng toàn cầu hơn là một sản phẩm khả dĩ của một chương trình nghiên cứu tiên tiến, tự chủ và chuyên biệt hay một phòng lab bí mật. Stuxnet cũng không có gì đặc biệt mới mẻ, sáng tạo. Khả năng xâm nhập các hệ thống bị cách ly đã trở thành tin cũ. Các hacker đã sử dụng kỹ thuật này để ăn trộm các tài liệu mật từ US CENTCOM (Bộ Chỉ huy Trung tâm Hoa Kỳ).

Tầm quan trọng chiến lược thực sự của Stuxnet nằm ở tầm nhìn mà nó mang lại về sự tiến hóa của chiến tranh máy tính vốn đang diễn ra cách xa Washington. Động lực của cuộc cách mạng này chính là giới tội phạm mạng công nghiệp. Hầu như tất cả các sự cố mạng lớn được báo cáo từ năm 2005 trở lại đây đều liên quan tới các thủ thuật, kỹ xảo và các mã gắn liền với giới tội phạm mạng. Các nhà chỉ trích đã cáo buộc Trung Quốc thuê ngoài các bên thứ ba vốn hoạt động ngoài vòng pháp luật tiến hành các cuộc tấn công ăn cắp bản quyền qua mạng chống lại Hoa Kỳ, hoặc ít nhất là Trung Quốc đã dựa vào hoạt động của các băng nhóm như vậy.[10] Các mạng máy tính ma (botnet) được quản lý bởi các nhóm tội phạm Nga đã tiến hành các cuộc tấn công từ chối dịch vụ (DDOS) làm gián đoạn các mạng quốc gia của Estonia vào tháng 5/2007. Các botnet này chính là một phần của một nền kinh tế ngầm bao gồm các tài nguyên và bộ phần mềm phục vụ tội phạm vốn được mua bán, trao đổi và thường được sử dụng cho các cuộc chiến giữa các công ty nhằm buộc các đối thủ cạnh tranh về kinh tế và chính trị bị loại ra khỏi thế giới mạng.

[10] Xem US–China Economic and Security Review Commission, *2009 Report to Congress*, November 2009, http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf; Alexander Klimburg, 'Mobilising Cyber Power', *Survival*, vol. 53, no. 1, February– March 2011, pp. 41–60

Các botnet đóng vai trò then chốt trong cuộc chiến năm 2008 giữa Nga và Gruzia, hỗ trợ Matxcơva trong vai trò một biện pháp nâng cao sức mạnh chiến lược khi tiến hành các chiến dịch quân sự thông qua các cuộc tấn công từ chối dịch vụ. Các botnet cấp độ thương mại có nguồn gốc từ Nga đã làm tắc nghẽn các website chính phủ Gruzia và giới truyền thông độc lập, đồng thời làm chính phủ nước này không thể liên lạc với người dân. Các cuộc tấn công từ chối dịch vụ giúp tạo ra một khoảng chân không thông tin làm tê liệt bộ máy hành chính của Gruzia. Trong mỗi trường hợp, Nga đều phủ nhận sự dính líu của mình. Tuy nhiên các cuộc tấn công botnet đã hỗ trợ chính sách nhà nước của Nga. Một điều tài tình của chiến lược này là không ai có thể chỉ ra mối liên hệ giữa chính phủ Nga với các cuộc tấn công mạng, giúp bảo vệ nhà nước Nga khỏi các cáo buộc chính trị và pháp luật.[11]

Trường hợp Gruzia và Estonia đại diện cho mô hình đang nổi lên. Các cuộc điều tra bởi cơ quan Giám sát Chiến tranh Thông tin về các cuộc tấn công *Ghostnet* và *Shadows* xuất phát từ Trung Quốc cho thấy các bộ phần mềm tội phạm nổi tiếng đã xâm nhập và ăn cắp các tài liệu mật từ cộng đồng người Tây Tạng lưu vong ở Ấn Độ như thế nào, cũng như cách chúng xâm nhập vào các mục tiêu cao như Bộ Quốc Phòng, Bộ Ngoại giao và các cơ sở nghiên cứu quốc phòng nước này ra sao.[12] Vụ xâm nhập quy mô lớn gần đây vào hệ thống thông tin mật tại CENTCOM dẫn tới sự thất thoát hàng ngàn tài liệu mật xảy ra khi một USB bị nhiễm một loại virus nổi tiếng đã vô tình được ai đó sử dụng trên một chiếc laptop có nối với mạng máy tính bảo mật.

Sự phổ biến của tội phạm trên không gian mạng mang lại một màn khói mù để che giấu các hoạt động gián điệp mạng. Đối với Stuxnet, một phần lớn các bằng chứng thu được – như các đoạn mã, quan hệ giữa các cá nhân, các mối tương quan trong không gian mạng – cho thấy có mối liên hệ giữa đoạn mã được sử dụng bởi Stuxnet với cộng đồng lập trình nước ngoài đang mở rộng của Nga, nơi các lập trình viên tài năng làm việc trên một thị trường chợ xám (grey market) buôn bán các đoạn mã. Trong cộng đồng này, không có sự phân biệt rạch ròi giữa các lập trình viên làm việc hôm nay với các thiết bị SCADA của Siemens (tức thiết bị điều khiển và quản lý các công trình công nghiệp, ví dụ như hệ thống điện lưới – ND) cho một khách hàng công nghiệp ở Saratov và ngày hôm sau làm lập trình online các phần mềm trò chơi cho một công ty game nước ngoài thuộc sở hữu của Israel nhưng đặt tại Ireland và Anh. Các mối liên hệ đều mù mờ, nhưng các dấu vết kỹ

[11] Ronald Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 South Ossetia War', bản thảo chuẩn bị xuất bản vào năm 2011.
[12] Xem http://www.infowar-monitor.net/.

thuật số trong không gian mạng không cho phép người ta ẩn danh hoàn toàn các đoạn mã hay địa điểm. Thông thường các mảnh ghép này có thể được ghép lại thành một bức tranh toàn cảnh, mặc dù việc tìm kiếm các câu trả lời rõ ràng thường rất phức tạp và khó khăn.

Stuxnet sử dụng các đoạn mã và kỹ xảo đã có sẵn. Điều này phục vụ hai mục đích. Thứ nhất, điều này giúp tiết kiệm chi phí bằng cách tận dụng các mã đã được chứng minh là hiệu quả. Như tổ chức Giám sát Chiến tranh Thông tin đã cho thấy trong các báo cáo về *Ghostnet* và *Shadows*, một mục tiêu có thể cùng lúc bị xâm phạm bởi một vài kẻ tấn công độc lập khác nhau đơn giản vì việc thiết kế và triển khai công nghệ không tốn kém, đồng thời có hiệu quả trên thực tế.

Thứ hai, việc sử dụng các cấu phần (đã có sẵn) của Stuxnet cho phép che dấu nguồn gốc của nó. Thách thức chủ chốt trong việc xác định các kẻ tấn công mạng nằm ở hệ sinh thái tối màu của không gian mạng. Việc xác định thủ phạm rất khó chứng minh. Liệu bên chịu trách nhiệm có phải là một hacker người Nga đang sinh sống ở New Zealand, người đã đóng góp một phần đoạn mã được sử dụng trong rootkit? Hay đó là một thiết bị trung gian đã chuyển đoạn mã cho một người nào đó làm việc trong cơ quan tình báo quân sự của nhà nước? Sự mù mờ có chủ đích chính là một chiếc khiên hiệu quả chống lại sự quy kết trách nhiệm.

Cách tiếp cận này cũng có cái giá của nó. Bất chấp tương đối phức tạp, Stuxnet đã nhanh chóng bị vô hiệu hóa một cách hiệu quả. Chỉ trong vài tháng các đặc tính kỹ thuật và cấu phần của nó đã được phơi bày. Iran đã có thể nhanh chóng tận dụng sức mạnh trí tuệ của cộng đồng an ninh mạng toàn cầu, mà về cơ bản là đã nhờ số đông để tìm giải pháp cho con sâu này, qua đó gây nghi ngờ cho những nhận thức lâu nay cũng như những tung hô về tính hiệu quả của các cuộc tấn công mạng. Việc Stuxnet nhanh chóng bị vô hiệu hóa cũng nêu lên câu hỏi tại sao cách tiếp cận này chứ không phải là một cách tiếp cận trực tiếp hoặc kín đáo hơn lại được chọn để nhằm vào chương trình hạt nhân của Tehran. Câu trả lời phụ thuộc vào các mục tiêu chính trị và chiến lược mà những kẻ tấn công đằng sau Stuxnet muốn nhắm tới.

Có nhiều đồn đoán cho rằng Israel hoặc có thể là Hoa Kỳ sẽ phát động các cuộc không kích nhằm trì hoãn chương trình hạt nhân của Iran trong suốt năm 2011, mặc dù có vẻ như Tổng thống Obama sẽ khó mà đồng ý cho phép tiến hành các cuộc không kích như vậy.[13] Các phí tổn và lợi ích của một hành động như vậy

[13] Ví dụ xem Jeffrey Goldberg, 'The Point of No Return', *Atlantic*, September 2010. Goldberg đã phỏng vấn một số người trong cuộc và báo cáo về điều mà ông cảm nhận là sự đồng thuận rằng Israel sẽ hành động.

đã được tranh luận rộng rãi.[14] Các tuyên bố gần đây của các lãnh đạo Ả-rập thể hiện quan ngại về mối đe dọa hạt nhân Iran đã mang lại cho lý do hành động của Israel một sự khả tín mới và tính chính đáng lớn hơn. Tiết lộ của WikiLeaks về các điện tín ngoại giao mật của Mỹ vào tháng 12/2010 đã củng cố sự tự tin của Tel Aviv. Các điện tín khẳng định rằng các lãnh đạo các nước láng giềng Ả-rập của Israel đồng ý với cảnh báo lâu nay của Thủ tướng Benjamin Netanyahu về khả năng hạt nhân ngày càng lớn mạnh của Iran.[15] Vua Ả-rập Xê-út Abdullah bin Abdulaziz đã nói với Mỹ rằng Mỹ cần "chặt cho rắn mất đầu". Tổng thống Ai Cập Hosni Mubarak đã gọi người Iran là "những kẻ nói dối trơ trẽn". Bộ trưởng Quốc phòng Các tiểu vương quốc Ả-rập Thống nhất đã so sánh Tổng thống Iran Mahmoud Admadinejad với Adolf Hitler. Vua Hamad Bin Isa Al Khalifa của Bahrain đã phát biểu rằng chương trình hạt nhân của Iran "phải được chặn đứng".[16] Vua Abdullah II của Jordan đã phát biểu trước công chúng vào đầu năm 2004, cảnh báo về sự xuất hiện của một "vòng cung người Shia" do Iran hậu thuẫn vốn có thể gây bất ổn cho Trung Đông.[17] Ông không kêu gọi tấn công Iran nhưng tình cảm muốn chặn bước Iran là rõ ràng.

Liệu một cuộc không kích chống lại chương trình hạt nhân của Iran có thành công hay không? Các cuộc không kích của Israel nhằm vào lò phản ứng Osirak của Iraq năm 1981 và một cơ sở của Syria vào năm 2007 đã thành công, nhưng chúng nhắm vào các vị trí đơn lẻ nằm trên mặt đất được phòng thủ nghèo nàn và gần với

---

[14] Gần đây nhất, xem Dana Allin and Steven Simon, *The Sixth Crisis: Iran, Israel, America and the Rumors of War* (New York: Oxford University Press, 2010); Steven Simon and Ray Takeyh, 'If Iran Came Close to Getting a Nuclear Weapon, Would Obama Use Force?', *Washington Post*, 1 August 2010; Kori Schake, 'Foreign Policy: Iran Sanctions Are Not Tough Enough', *Foreign Policy*, 10 June 2010; Trita Parsi, 'Want to Defuse the Iran Crisis?', *Foreign Policy*, 12 November 2010; Goldberg, 'The Point of No Return'; Dan Murphy, 'Could an Israeli Air Strike Stop Iran's Nuclear Program?', *Christian Science Monitor*, 13 October 2009; Scott Peterson, 'Iran War Games Begin with "Ultra Fast" Speed Boats', *Christian Science Monitor,* 22 April 2010; Robert D. Kaplan, 'Living with a Nuclear Iran', *Atlantic*, September 2010; and Sam Gardiner, *The Israeli Threat: An Analysis of the Consequences of an Israeli Air Strike on Iranian Nuclear Facilities* (Stockholm: Swedish Defence Research Agency, March 2010).

[15] Về các tuyên bố của Netanyahu, xem Dan Murphy, 'Repercussions of an Israeli Attack on Iran', *Christian Science Monitor*, 12 August 2010.

[16] Ian Black and Simon Tisdall, 'Saudi Arabia Urges US Attack on Iran to Stop Nuclear Programme', *Guardian*, 29 November 2010; 'WikiLeaks and Israel – Quiet Relief, Louder Vindication, for Now', *Los Angeles Times*, 29 November 2010; Andrea Stone, 'WikiLeaks: Arabs Agree that Iran is a Threat', AoLNews.com, 29 November 2010, http://www.aolnews.com/2010/11/29/wikileaks-arabs-agree-with-israelthat-iran-is-a-threat/.

[17] Abbas Kadhim, 'Shi'a Perceptions of the Iraq Study Group Report', *Strategic Insights*, vol. 6, no. 2, March, 2007; Ian Black, 'Fear of a Shia Full Moon', *Guardian*, 26 January 2007. Xem thêm Bob Woodward, *The War Within* (New York: Simon and Schuster, 2008), pp. 258–9, cuốn sách này cho thấy các lo ngại chống lại Iran không phải là điều mới mẻ. Tác giả báo cáo rằng các bộ trưởng Hội đồng Hợp tác vùng Vịnh đã thể hiện sự lo lắng với Ngoại trưởng Hoa Kỳ Condoleezza Rice về mối đe dọa mà họ cảm nhận những người Hồi giáo dòng Shi'ite sẽ đặt ra với người Hồi giáo dòng Sunni tại khu vực.

Israel. Các mục tiêu ở Iran nằm cách xa hơn nhiều. Các tiết lộ của Wikileaks cho thấy Ả-rập Xê-út có thể cho phép bay qua lãnh thổ của mình. Hoa Kỳ rõ ràng cũng sẽ cho phép Israel bay qua Iraq.[18] Các bom phá boong-ke của Israel có thể xuyên phá các công trình ngầm như Natanz. Mặc dù các hạn chế về tiếp liệu sẽ có thể ngăn cản Israel tấn công toàn bộ các cơ sở hạt nhân của Iran trong một vụ không kích đơn lẻ, các máy bay của nước này vẫn có thể tấn công các địa điểm chính vốn thiết yếu cho việc sản xuất nguyên liệu phân hạch. Bất chấp những lời khoe mẽ, hệ thống phòng không của Iran vẫn tỏ ra đáng ngờ. Thành công sẽ giúp Israel đạt được các mục tiêu an ninh trọng yếu và giúp ngăn ngừa một cuộc chạy đua vũ trang hạt nhân trong khu vực.

Nhưng một cuộc không kích cũng đặt ra các rủi ro. Một cuộc không kích duy nhất có thể không thành công, và cũng không rõ Ả-rập Xê-út hay Hoa Kỳ sẽ cho phép bao nhiêu chuyến bay quá cảnh. Israel có thể gánh chịu những tổn thất đáng kể. Iran sẽ buộc Hoa Kỳ chịu trách nhiệm, và có thể tấn công các cơ sở và binh lính của Mỹ ở Iraq, Afghanistan và các nơi khác. Nước này cũng có thể gián đoạn nguồn cung dầu mỏ chảy từ vùng Vịnh và giá dầu có thể leo thang. Các cuộc không kích có thể giúp đoàn kết một Iran hiện đang bị chia rẽ và giúp Admadinejad và các đồng minh củng cố quyền lực.

Vậy liệu một cuộc tấn công mạng có mang lại một biện pháp đánh đổi rủi ro - lợi ích tốt hơn nhằm đạt được mục tiêu ngăn chặn hoặc làm chậm lại chương trình hạt nhân của Iran hay không? Stuxnet đã hoạt động thành công tới mức nào? Thoạt tiên, Bộ trưởng Truyền thông Iran Reza Taghipour đã phủ nhận. Ông ta tuyên bố rằng "tác động và thiệt hại của virus gián điệp này trong các hệ thống máy tính chính phủ là không nghiêm trọng", và rằng "hầu hết mọi khu vực bị tác động đã được xác định và xử lý".[19] Sau đó, Ahmadinejad thừa nhận rằng Stuxnet đã làm trì hoãn chương trình nhưng nó chỉ tác động vào một "số lượng hạn chế các máy ly tâm".[20] Siemens thừa nhận rằng Stuxnet đã tấn công vào 14 nhà máy công

[18] Goldberg, 'The Point of No Return'.
[19] Scott Lucas, 'Is the Stuxnet Worm a State-directed Cyber-attack on Iran?', *EAWorldView,* 26 September 2010, http://www.enduringamerica.com/home/2010/9/26/is-the-stuxnet-worma-state-directed-cyber-attack-on-iran.
html, trích dẫn lời hãng tin bán chính thức Mehr News Agency; 'Iran Identifies Sources of Stuxnet Virus in its Computers', Radio Samaneh/Payvand.com, 21 October 2010, http://www.payvand.com/news/10/oct/1169.html.
[20] Gautham Nagesh, 'Iran Says Stuxnet Damaged its Nuclear Program', The Hill, 29 November 2010, http://thehill.com/blogs/hillicon-valley/technology/130965-iran-says-stuxnetdamaged-its-nuclear-program.

nghiệp, cả ở trong và ngoài Iran. Tehran đã khăng khăng rằng không có hoạt động của nhà máy Iran nào bị tác động nghiêm trọng.[21]

Tuy nhiên, các thanh sát viên Cơ quan Năng lượng Nguyên tử Quốc tế (IAEA) đã báo cáo rằng Iran đã dừng đưa uranium vào các máy ly tâm ở Natanz trong một tuần vào cuối tháng 11, đây có thể là chỉ dấu cho thấy một sự hư hỏng lớn.[22] Mức giảm 23% số máy ly tâm hoạt động từ giữa năm 2009 tới giữa năm 2010 có thể là do bị Stuxnet tấn công.[23] Phạm vi đầy đủ của sự phá hoại vẫn cần thời gian để làm rõ nhưng người Iran rõ ràng đã chủ quan và bị bất ngờ bởi mức độ mà hệ thống phòng thủ của họ bị xâm nhập, ngay cả đối với các hệ thống cách ly được bảo vệ cẩn mật. Và ngay cả khi các thiệt hại là không lớn và được khắc phục nhanh chóng thì Stuxnet vẫn chỉ ra một con đường mới phía trước. Một cuộc tấn công tương lai sửa dụng các sâu máy tính hoặc các malware phức tạp hơn có thể gây nên những thiệt hại nghiêm trọng và kéo dài hơn.

Các quy chuẩn đang nổi lên

Iran đã gọi Stuxnet là một sự thất bại. Không có bằng chứng nào chỉ ra ai là người thực hiện các cuộc xâm nhập và gây gián đoạn, và nếu chúng ta chấp nhận thông tin của Iran về các thiệt hại thì khó lòng nói rằng Stuxnet đại diện cho một sự sử dụng vũ lực, một cuộc tấn công vũ trang hay một cuộc xâm lược theo định nghĩa của Hiến chương Liên Hiệp Quốc.[24] Một nghị quyết của Đại Hội đồng năm 1974 đã định nghĩa "xâm lược" bao gồm hành động "oanh tạc bởi các lực lượng vũ trang của một Nhà nước chống lại lãnh thổ của một nhà nước khác hoặc *việc sử dụng bất cứ vũ khí gì của một Nhà nước chống lại lãnh thổ của một Nhà nước khác*".[25] Nhưng nghị quyết ra đời trước khi chiến tranh mạng xuất hiện. Liệu các cơ sở công nghiệp có được coi là "lãnh thổ" hay không vẫn chưa rõ, nhưng chúng ta có thể lập luận một cách hợp lý rằng hành động xâm lược bao gồm cả việc sử dụng các vũ khí mạng vốn có thể gây nên thiệt hại đối với tài sản hoặc làm con người bị thương.

[21] McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems'.
[22] William J. Broad, 'Reports Suggests Problems with Iran's Nuclear Effort', *New York Times*, 23 November 2010.
[23] John Markoff and David E. Sanger, 'In a Computer Worm, a Possible Biblical Clue', *New York Times*, 29 September 2010.
[24] Khái niệm "sử dụng vũ lực" theo Điều 2(4) và "tấn công vũ trang" theo điều 51 của Hiến chương Liên Hiệp Quốc có mối liên hệ với nhau cũng như với khái niệm "xâm lược".
[25] UN General Assembly Resolution 3314 (XXIX), Article 3(b), http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf.

Không quân Hoa Kỳ định nghĩa vũ khí là "các thiết bị được thiết kế để giết, làm bị thương, gây tàn tật cho con người hoặc gây thiệt hại hoặc phá hủy tài sản."[26]

Nhưng khi nào thì tấn công mạng được coi như việc sử dụng vũ lực hoặc tấn công vũ trang? Phần lớn thừa nhận rằng điều này phụ thuộc vào các hoàn cảnh và hậu quả xảy ra. Các cuộc tấn công mạng nào gây nên thiệt hại vật chất hoặc làm con người bị thương giống như thiệt hại hay thương vong trong các cuộc chiến tranh thông thường thì được coi là tương đương với việc sử dụng vũ lực và tấn công vũ trang.[27] Ngắt nguồn điện khỏi các cơ sở kiểm soát không lưu và khiến máy bay bị rơi sẽ được coi như là hành động sử dụng vũ lực cho dù cuộc tấn công chỉ là một dạng từ chối dịch vụ đối với các hệ thống máy tính, làm gián đoạn chức năng của chúng, hoặc việc tiêm nhiễm các virus, sâu máy tính hoặc các malware nhằm đạt được kết quả tương tự.

Các cuộc tấn công mạng nào gây nên các thiệt hại vật chất có thể khắc phục được mà không tạo ra hậu quả lâu dài và không làm con người bị thương thì không được coi như là việc sử dụng vũ lực và tấn công vũ trang. Ví dụ, đây là cách nhìn nhận đối với hàng nghìn các sựu cố thăm dò tìm thông tin về mạng (probes) hay xâm nhập mạng (penetrations) chống lại Bộ Quốc phòng Hoa Kỳ.[28] Nhưng việc hạ bệ các hạ tầng trọng yếu như hệ thống tài chính của một quốc gia, hay gây nên gián đoạn nghiêm trọng đối với thương mại, nền kinh tế, việc làm và cuộc sống thì có được coi tương đương với sử dụng vũ lực hay không? Nếu xét trên khía cạnh chính trị thực tiễn thì các công dân và chính phủ các nước phương Tây sẽ phản ứng như thế nào nếu các thể chế tài chính của họ bị đánh sập mạng? Việc đánh sập các cơ quan này thông qua tấn công mạng khác gì với hành động tương tự thông qua các cuộc tấn công tên lửa? Câu trả lời đối với nhiều câu hỏi như vậy mặc dù vậy lại bị chi phối bởi các cân nhắc chính trị, ngoại giao và chiến lược hơn là các cuộc tranh luận sáo rỗng về các quy tắc của luật pháp quốc tế.

Hoa Kỳ coi không gian mạng như một không gian tác chiến vốn thiên về tấn công. Chính sách Hoa Kỳ rõ ràng tìm cách chiếm ưu thế trong không gian này. Hoa

---

[26] US Department of the Air Force, 'Compliance with the Law of Armed Conflict', Policy Directive 51-4, 1993, para. 6.5.

[27] William A. Owens, Kenneth W. Dam and Herbert S. Lin (eds), *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington DC: National Academies Press, 2009), p. 251 và Appendix D, p. 356.

[28] Một báo cáo đệ trình lên Quốc Hội Hoa Kỳ năm 2009 cho rằng vào năm 2008, 54.640 cuộc tấn công mạng đã được tiến hành chống lại Bộ Quốc phòng Hoa Kỳ, tăng vọt so với con số 43.880 vụ năm 2007. Tướng John Davis, phó tư lệnh phụ trách tác chiến mạng tại Bộ Chỉ huy Mạng Hoa Kỳ tuyên bố rằng chỉ trong sáu tháng đầu năm 2009, quân đội đã chi 100 triệu đô la để sửa chữa các thiệt hại của các mạng gây nên bởi các cuộc tấn công mạng. Mặc dù các mối quan ngại ngày càng tăng nhưng không có bên nào bị buộc tội tiến hành tấn công vũ trang chống lại Hoa Kỳ. Xem US–China Economic and Security Review Commission, *2009 Report to Congress*,p. 168.

Kỳ không đưa ra chính sách được tuyên bố nào đối với các vũ khí mạng,[29] nhưng Trung tướng Keith Alexander, tư lệnh của Bộ tư lệnh Mạng mới được bổ nhiệm, lại làm rõ rằng Hoa Kỳ có quyền đáp trả lại qua không gian mạng một cuộc tấn công mạng nhắm vào các hệ thống của Bộ Quốc phòng.[30] Cách tiếp cận của chính quyền Obama mang tính đa phương, một báo cáo rà soát chính sách tuyên bố rằng "chỉ bằng cách làm việc với các đối tác quốc tế Hoa Kỳ mới có thể giải quyết tốt nhất các thách thức [an ninh mạng]".[31] Nước Anh đã kêu gọi việc điều phối quốc tế về chiến lược an ninh mạng trong khi vẫn đảm bảo được ưu thế trong không gian ảo.[32]

Stuxnet có thể đại diện cho một biến đổi mới: đó là việc sử dụng lần đầu tiên một vũ khí mạng được bao bọc trong sự mù mờ bằng cách sử dụng các tài nguyên có sẵn và có thể bác bỏ được vốn được lấy từ cộng đồng tội phạm mạng toàn cầu nhằm giúp tránh bị quy kết trách nhiệm. Nhưng quy kết trách nhiệm chỉ là một vấn đề về cách giải thích. Việc áp dụng hiện tại trên thực tế một tiêu chuẩn bất lợi về bằng chứng có nghĩa là các quốc gia có thể lảng tránh trách nhiệm ngay cả đối với các sự cố xảy ra trong một phần không gian mạng mà quốc gia đó có thẩm quyền quản lý về chủ quyền hay quyền tài phán. Luật về Xung đột Vũ trang truyền thống đòi hỏi phải xác định được kẻ tấn công. Trong chiến tranh mạng sẽ khó có thể làm được điều đó. Ngay cả khi các cuộc tấn công xuất phát từ bên ngoài, ở ngoài quốc gia bị nhắm tới, thì vẫn còn những câu hỏi lớn về trách nhiệm của nạn nhân trong việc xác định địa điểm vật lý của một máy tính hay một mạng máy tính. Như Herbert Lin, khoa học trưởng tại Ban Viễn thông và Khoa học Máy tính của Hội đồng Nghiên cứu Quốc gia Hoa Kỳ đã chỉ ra:

> Anh có thể có chỉ một địa chỉ IP, không phải là một địa điểm vật lý mà anh có thể tấn công trả thù. Giả dụ như có một máy tính điều khiển mạng lưới phòng không của đối phương và anh không thể xác định được vị trí địa lý của nó. Nếu anh truy lùng nó thông qua một cuộc tấn công mạng, thì điều gì sẽ xảy ra nếu chiếc máy tính đó nằm ở một quốc gia trung lập? Hay nằm ngay trên chính

[29] Xem Peter Pace, 'National Military Strategy for Cyber Space Operations', unclassified memo, December 2006, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf; *Cyberspace Operations*, Air Force Doctrine Document 3-12, 15 July 2010, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf.

[30] 'Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command', http://armedservices.senate.gov/statemnt/2010/04April/Alexander 04-15-10.pdf, pp. 19, 24.

[31] White House, 'Cyberspace Policy Review', May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, p. 20.

[32] 'Cyber Security Strategy of the United Kingdom – Safety, Security and Resilience in Cyber Space', UK Cabinet Office, June 2009.

> lãnh thổ của anh? Chiến tranh mạng làm phức tạp hóa các vấn đề và thách thức các khái niệm truyền thống về sự trung lập và chủ quyền.[33]

Hơn nữa, việc một mạng botnet được sử dụng để tấn công Estonia và Gruzia có thể bao gồm các máy tính đặt tại Châu Âu và Hoa Kỳ sẽ không quan trọng bằng thực tế rằng các lệnh điều khiển, hoặc các hướng dẫn cho các mạng kiểm soát và điều khiển lại xuất phát từ các địa chỉ IP nằm trong Liên bang Nga.

Thay đổi các tiêu chuẩn về quy kết trách nhiệm sẽ thay đổi các giới hạn hiện tại đang đặt không gian mạng ra ngoài vòng pháp luật về xung đột vũ trang và luật pháp quốc tế, đồng thời đưa nó vào vị trí được điều chỉnh bởi Hiến chương Liên Hiệp Quốc. Việc này cũng sẽ khiến cho không gian mạng nhất quán với Chiến lược An ninh Quốc gia của Hoa Kỳ vốn từ sau sự cố 11/9 đã buộc trách nhiệm đối với các quốc gia chứa chấp những kẻ phát động tấn công, đồng thời cho phép Hoa Kỳ có quyền thực hiện tấn công phủ đầu để ngăn chặn, răn đe hoặc phá hủy cuộc tấn công đó. Một sự thay đổi như vậy sẽ làm nổi bật vấn đề liệu một sự phản ứng thông qua không gian mạng có mang lại một lựa chọn được áp dụng đầu tiên hay cuối cùng và đáp ứng được các tiêu chí về sự cần thiết và mức độ tương xứng theo luật pháp quốc tế hay không. Như Lin chỉ ra, những vấn đề này khi áp dụng vào không gian mạng vẫn còn chưa được kiểm chứng: "Đây là một lãnh địa mới và đòi hỏi tư duy mới khi các quốc gia phát triển các chính sách cho tương lai để chống lại và bảo vệ mình trước các cuộc tấn công mạng."[34]

Các quốc gia phản ứng như thế nào, và mức độ ủng hộ mà họ tạo ra trong việc tự vệ chống lại một cuộc tấn công là bao nhiêu, tất cả phụ thuộc vào sức mạnh và tầm quan trọng tương đối của họ. Ví dụ, vào năm 2007, thách thức đó đã đã hiện diện trước Estonia, nước đã cáo buộc Nga tiến hành các cuộc tấn công từ chối dịch vụ gây tê liệt.[35] Là một thành viên NATO, Estonia tìm cách kêu gọi việc phòng thủ tập thể theo Điều V của Hiến chương Đại Tây Dương. Tuy nhiên, NATO đã từ chối cáo buộc Nga thực hiện tấn công vũ trang. Vị Bộ trưởng Quốc phòng thất vọng của Estonia Jaak Aaviksoo đã so sánh cuộc tấn công từ chối dịch vụ với một hoạt động khủng bố. Tallinn tuyên bố rằng tấn công từ chối dịch vụ chống lại các mạng quốc gia được phối hợp bởi các máy tính đặt trong không gian mạng của Nga và ít nhất nhận được sự đồng ý công khai của giới chức nước này. Trong các hoàn cảnh khác, điều này có thể thỏa mãn tiêu chí mà dựa vào đó NATO xác định một cuộc

[33] Phỏng vấn với Dr. Herbert Lin.
[34] Như trên.
[35] Xem Ian Traymor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *Guardian*, 17 May 2007; 'NATO Says Urgent Need to Tackle Cyber Attack', Reuters, 21 June 2007; Evgeny Morozov, 'The Fog of Cyberwar', *Newsweek*, 18 April 2009.

tấn công vũ trang đã xảy ra mặc dù đáng kể là không có thiệt hại vĩnh viễn nào đối với tài sản hay thương vong nào đối với con người xảy ra. Aaviksoo thừa nhận rằng cả EU và NATO đã không định nghĩa "điều gì có thể được coi như là một cuộc tấn công mạng hoặc đâu là quyền của các nước thành viên và đâu là nghĩa vụ của EU và NATO nếu các cuộc tấn công như vậy được tiến hành".[36] Ông nói thêm rằng "NATO không định nghĩa các cuộc tấn công mạng là một hành vi quân sự rõ ràng. Điều này có nghĩa là các quy định của Điều V …sẽ không tự động được áp dụng."[37]

Việc vận dụng tấn công mạng bởi các quốc gia vẫn còn hạn chế. Nhưng rõ ràng như trong trường hợp Stuxnet, nó nêu lên vấn đề liệu hành động này có được biện minh theo Hiến chương Liên Hiệp Quốc hay không? Liệu cuộc tấn công có phải là một hành động tự vệ chống lại một mối đe dọa hiện hữu và rõ ràng, như những người ủng hộ việc chấm dứt chương trình hạt nhân của Iran sẽ có thể lập luận, hay đó chỉ là một cuộc tấn công vũ trang không được biện minh cũng như việc can thiệp không được phép vào công việc nội bộ của một quốc gia khác, vốn bị cấm theo Điều 2(4) của Hiến chương?

Mức độ tương xứng đặt ra một giới hạn khác. Quyền phát động chiến tranh – *jus ad bellum* – đòi hỏi một sự phản ứng tương xứng nhằm tránh thiệt hại không chủ đích. Như thế nào là một sự phản ứng tương xứng là một đoán định mang tính chủ quan cố hữu. Điều này quan trọng đối với các quốc gia muốn hành động của mình được coi là hợp pháp. Nhưng nó có thể không quan trọng đối với một quốc gia không quan tâm điều đó, hoặc khi bị tấn công, muốn gửi một thông điệp răn đe tương lai mạnh mẽ đối với kẻ tấn công.

Vấn đề của việc phụ thuộc vào Liên Hiệp Quốc là ở chỗ quy trình nếu đưa lên Liên Hiệp Quốc sẽ chậm chạp, bị chi phối bởi tính chính trị và hầu như vô ích khi đối mặt với các cuộc tấn công thời gian thực. Nhưng điều này mang lại một kênh để thảo luận, tố cáo, và thậm chí là hành động, điều vốn có thể hữu ích về mặt ngoại giao đối với các vấn đề lâu dài. Iran sẽ thấy Hội đồng Bảo an ít có giá trị trong việc ứng phó với Stuxnet. Xác suất của việc Iran giành được một nghị quyết ủng hộ lập trường của mình là bằng không. Câu hỏi thú vị hơn là lợi ích mà quốc gia phải chịu thiệt hại không chủ đích sẽ có được là gì? Có lẽ lợi ích đó là sử dụng áp lực đối với những nước dùng tấn công mạng nhằm hạn chế các chiến dịch trong tương lai, qua đó giúp tránh được các thiệt hại như vậy.

Cuộc tranh luận về việc sâu Stuxnet – hoặc một phiên bản tương lai nguy hiểm hơn – có được coi là việc sử dụng vũ lực hay một cuộc tấn công vũ trang

[36] Traymor, 'Russia Accused of Unleashing Cyberwar'.
[37] Như trên.

không sẽ dẫn chúng ta tới đâu? Israel và Mỹ sẽ lập luận rằng hành động nhằm trì hoãn hoặc phá hủy các cơ sở hạt nhân của Iran là một hành động tự vệ chống lại một mối đe dọa hiện hữu, do đó không bị cấm đoán và giúp ngăn ngừa một cuộc chạy đua vũ trang có thể mang tính hủy diệt, cho nên hành động đó được cho phép theo Điều 51 của Hiến chương.[38] Iran sẽ lập luận rằng các diễn dịch này vượt quá phạm vi thông thường của khái niệm tự vệ và rằng Stuxnet là một sự can thiệp bị cấm đoán vào công việc nội bộ của nước này. Dù khẳng định quyền được phát triển năng lượng hạt nhân một cách hòa bình, Iran đã bác bỏ bất cứ ý định nào trong việc chế tạo vũ khí hạt nhân, mặc dù các máy ly tâm ở Natanz sẽ khó giải thích trừ việc chúng là một phần nỗ lực nhằm đạt được ít nhất là ngưỡng năng lực vũ khí hạt nhân.[39] Iran cũng có thể lập luận rằng mục tiêu của nước này hoàn toàn mang tính phòng thủ và không tạo ra một mối đe dọa nào đối với những quốc gia không xâm lược.

Kết luận

Vẫn chưa rõ thiệt hại vật chất phải ở mức bao nhiêu thì mới được coi là tương đương với việc sử dụng vũ lực. Về vấn đề quy mô, Lin đặt câu hỏi: "Liệu có (hay nên có) một dạng tấn công mạng mà dù quy mô hạn chế cũng được coi như việc sử dụng vũ lực, và cho phép đối tượng bị tấn công có thể có hành động nào đó để tự vệ mà đi xa hơn việc đơn thuần bảo vệ mục tiêu trước mắt hay không?".[40] Cũng có một câu hỏi phụ là liệu một cuộc tấn công có ý định nhưng không thành công trong việc tạo ra thiệt hại lớn hơn thì có được xếp vào loại này hay không. Hàm ý của những kịch bản này minh họa cho sự phức tạp mà tấn công mạng đặt ra cho tương lai. Tấn công mạng rất khó chấm dứt và các hacker đã chứng minh internet là một kênh lý tưởng để chèn các malware (vào các hệ thống mục tiêu). Đó là lý do tại sao nhiều người ủng hộ việc tách các hạ tầng trọng yếu ra khỏi internet hoặc đặt ra các giao thức an ninh nghiêm ngặt để ngăn ngừa xâm nhập. Stuxnet thêm vào một vấn đề cụ thể: rõ ràng một số máy tính bị nhiễm virus thông qua USB. Thực hiện điều này đòi hỏi hiểu biết về lĩnh vực chuyên môn. Báo chí cho rằng có

[38] Ví dụ, xem W. Michael Reisman, 'Criteria for the Lawful Use of Force in International Law', *Yale Journal of International* Law, vol. 10, 1985, pp. 279, 281; W. Michael Reisman, 'The Use of Force in Contemporary International Law', *American Society of International Law Proceedings*, vol. 78–79, 1984–85, pp. 79–84; W. Michael Reisman, 'War Powers: The Operational Code of Competence', *American Journal of International Law*, vol. 83, 1989, p. 777; Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', *Columbia Journal of Transnational Law*, vol. 37, 1999, p. 885.

[39] 'Iran's Rights to Nuclear Nonnegotiable: Ahmadinejad', *Reuters,* 10 November 2010; 'Ahmadinejad: Iran is Now a "Nuclear State"', Associated Press*,* 11 February 2010.

[40] Phỏng vấn với Dr Herbert Lin.

người làm tay trong tại một cơ sở hạt nhân nào đó của Iran, nhưng đó có thể là một kết luận vội vàng. Stuxnet đã nhiễm vào nhiều máy tính ở nhiều nước khác nhau, và vẫn chưa hoàn toàn rõ ràng con sâu này đã được phát tán như thế nào.

Các cuộc tấn công mạng có rủi ro tạo ra các thiệt hại không chủ đích. Là một nhà máy chứa các máy ly tâm có thể được sử dụng để chế tạo uranium cấp độ vũ khí, Natanz đáp ứng tiêu chuẩn của một mục tiêu quân sự đúng nghĩa. Các tài sản ở các quốc gia khác mà Stuxnet không định tấn công thì không. Rõ ràng Stuxnet đã phá hủy tài sản của một số quốc gia bên ngoài Iran, nước chỉ chiếm 60% trường hợp nhiễm Stuxnet. Một số thiệt hại ở các nước như Ấn Độ, vốn có một vệ tinh bị ảnh hưởng, có thể nghiêm trọng. Điều này tạo nên rủi ro nghiêm trọng tiềm tàng về đáp trả chính trị nếu bên tiến hành tấn công được nhận diện.

Một vụ tấn công mạng được tiến hành tốt mang lại cơ hội để xác định mục tiêu một cách tinh vi. Nhưng nếu thiệt hại từ các vụ tấn công mạng có thể được khắc phục một cách nhanh chóng thì các cân nhắc chiến lược cẩn thận cần được đưa ra để so sánh chi phí và lợi ích của tấn công mạng so với tấn công quân sự truyền thống. Chắc chắn một lợi ích quan trọng của tấn công mạng là cơ hội cao hơn trong việc đạt được các mục tiêu như làm chậm lại chương trình hạt nhân của Iran mà không gây nên thương vong cho những người dân thường vô tội mà các cuộc không kích nhiều khả năng sẽ gây ra.

Khó khăn trong việc xác định thủ phạm tấn công mạng gây nên nhiều rắc rối cho việc phản ứng lại. Các quốc gia như Iran và Israel sẽ hành động để bảo vệ lợi ích của họ, nhưng họ sẽ muốn cộng đồng quốc tế thừa nhận tính hợp pháp của hành động mà họ thực hiện. Luật về Xung đột Vũ trang và Điều 51 thực tế đều yêu cầu hành động tự vệ phải dựa trên việc chứng minh được danh tính kẻ tấn công. Không rõ là mức độ chắc chắn trong việc nhận diện này đến mức độ nào thì có thể đưa ra được phản ứng. Tiến hành một hành động phản ứng chống lại một bên vô tội sẽ tương đương với hành động xâm lược, chứ không phải tự vệ. Tuy nhiên, trong trường hợp này các blogger người Israel đã ca ngợi sự tham gia của nước này. Điều này giúp làm rõ thủ phạm, giảm gánh nặng cho Iran nếu Iran chọn cách trả đũa.

Mặc dù không có bằng chứng rõ ràng cho thấy Stuxnet đã khiến Ahmadinejad bị công luận chỉ trích rằng chính phủ đã không thể bảo vệ các hạ tầng trọng yếu một cách hiệu quả, nhưng không gian mạng vẫn có thể là một công cụ để làm mất uy tín, gây bất ổn và làm suy yếu chính quyền của các chế độ đối địch. Không gian mạng cũng mang lại khả năng lớn nhằm tấn công các kẻ thù với rủi ro thấp hơn so với sử dụng các công cụ quân sự truyền thống. Ví dụ, Bắc Triều Tiên

gây nên các mối đe dọa khác nhau ngoài chương trình hạt nhân của nước này, ví dụ như việc làm tiền giả quy mô lớn. Tấn công mạng mang lại các lựa chọn tỏ ra hiệu quả trong việc đáp lại những hành động tội phạm như vậy. Hơn nữa, không gian mạng lại ít tốn kém hơn so với hành động quân sự truyền thống. Chưa rõ Stuxnet mất bao nhiêu chi phí để lập trình, nhưng gần như chắc chắn là nó rẻ hơn so với chi phí của một chiếc máy bay ném bom.

Các bên thứ ba hiện đang cộng tác với một nhà nước có thể hoặc không thể bị kiểm soát một cách chặt chẽ. Các nhóm tội phạm giống như lính đánh thuê. Họ có thể bán các dịch vụ của mình hai lần. Thuê ngoài giới tội phạm ngầm là một việc làm rủi ro. Tuy nhiên, về mặt trái, sự tiến hóa của các chiến lược mạng có thể gây bất lợi cho Hoa Kỳ so với các quốc gia khác khi thuê ngoài các bên thứ ba tiến hành các cuộc tấn công mạng hoặc dựa vào họ để đối phó với các mối đe dọa mạng. Luật chống Lạm dụng và Lừa đảo Máy tính[41] đã đặt ra các hạn chế nghiêm ngặt đối với khả năng của Hoa Kỳ trong việc thuê ngoài các hoạt động mạng, ít nhất là nếu thuê các công dân Hoa Kỳ.

Cuối cùng, một rủi ro chiến lược trọng yếu của tấn công mạng nằm ở chỗ khả năng diễn ra leo thang các hành động đáp trả. Các quốc gia như Iran và Bắc Triều Tiên được cho là có khả năng tiếp cận các năng lực mạng tinh vi. Các cuộc tấn công mạng hiệu quả bởi các quốc gia như vậy lên các hạ tầng trọng yếu có thể tạo ra những vấn đề lớn. Vấn đề quy trách nhiệm kẻ tấn công mà Iran gặp phải trong trường hợp Stuxnet sẽ làm hạn chế khả năng của các quốc gia khác trong việc đáp trả, đặc biệt là nếu xét đến số lượng cực lớn các cuộc tấn công mạng mà các nước phương Tây đã gánh chịu. Chúng ta có thể tỏ ra dễ bị tổn thương hơn so với các nước đó. Thực tế, một báo cáo gửi lên Quốc hội vào giữa tháng 12 đã cảnh báo rằng Stuxnet có thể được điều chỉnh kết hợp vào một loại vũ khí có thể gây nên thiệt hại rộng khắp cho các hạ tầng trọng yếu ở Hoa Kỳ.[42] Các chiến lược sử dụng các vũ khí mạng như Stuxnet cần phải cân nhắc thực tế rằng đối thủ có thể cố gắng sử dụng chúng để chống lại chính chúng ta.[43]

---

[41] 18 USC 1030, amended in 1988, 1994, 1996, 2001 (by the USA Patriot Act), 2002 and 2008 (by the Identify Theft Enforcement and Restitution Act), Luật quy định mức phạt nghiêm khắc lên các bên người Hoa Kỳ nào gây nên ít nhất 5.000 đô la Mỹ thiệt hại đối với máy tính của một bên khác.

[42] Paul K. Kerr, John Rollins and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, CRS Report for Congress R41524 (Washington DC: Congressional Research Service, 9 December 2010).

[43] Mark Clayton, 'Stuxnet "Virus" Could Be Altered to Attack U.S. Facilities, Report Warns', *Chrisian Science Monitor*, 15 December 2010.

GIỚI THIỆU DỰ ÁN *NGHIENCUUQUOCTE.NET*

Mục đích

Nghiencuuquocte.net là một dự án phi chính trị, phi lợi nhuận nhằm mục đích phát triển nguồn học liệu chuyên ngành nghiên cứu quốc tế bằng tiếng Việt và thúc đẩy việc học tập, nghiên cứu các vấn đề quốc tế tại Việt Nam.

Lý do ra đời

Trong khi số người học tập và nghiên cứu về các vấn đề quốc tế ở Việt Nam ngày càng gia tăng thì việc tiếp cận các tài liệu mang tính học thuật của thế giới về lĩnh vực này còn rất hạn chế vì hai lý do: Thứ nhất, các tài liệu này thường phải trả phí mới tiếp cận được, trong khi các trường đại học và viện nghiên cứu của Việt Nam hầu như không có chi phí trang trải. Thứ hai, các tài liệu này chủ yếu được xuất bản bằng tiếng Anh, khiến nhiều sinh viên, nhà nghiên cứu, và đặc biệt là quảng đại độc giả quan tâm đến các vấn đề quốc tế nói chung, gặp khó khăn trong việc tiếp thu, lĩnh hội. *Nghiencuuquocte.net* ra đời với hi vọng sẽ góp phần khắc phục được các vấn đề trên.

Hoạt động chính

Hoạt động chính của *Nghiencuuquocte.net* là biên dịch sang tiếng Việt và xuất bản trên website của mình các nguồn tài liệu mang tính học thuận bằng tiếng Anh về lĩnh vực quan hệ quốc tế, bao gồm chính trị quốc tế, kinh tế quốc tế, và luật pháp quốc tế.
Các tài liệu này chủ yếu là các bài báo trên các tập san quốc tế, các chương sách, hoặc các tài liệu tương ứng, đã được xuất bản bởi các nhà xuất bản, các trường đại học và viện nghiên cứu có uy tín trên thế giới.

Dự án ưu tiên biên dịch và xuất bản:

- Các bài viết mang tính nền tảng đối với lĩnh vực nghiên cứu quốc tế;
- Các bài viết có nhiều ảnh ảnh hưởng trong lĩnh vực này;
- Các bài viết liên quan trực tiếp hoặc có ảnh hưởng, hàm ý gián tiếp đến Việt Nam;
- Các bài viết được đông đảo độc giả quan tâm.

Trang chủ dự án: http://nghiencuuquocte.net/
Thông tin thêm về Dự án: http://nghiencuuquocte.net/about/
Danh mục các bài đã xuất bản: http://nghiencuuquocte.net/muc-luc/
Theo dõi Dự án trên Facebook: https://www.facebook.com/DAnghiencuuquocte

Ý kiến đóng góp và mọi liên hệ xin gửi về: Lê Hồng Hiệp, nghiencuuquocte@gmail.com