Nỗ lực chiến tranh mạng của tq lớn chưa từng thấy
Đường Thư

Một bản điều tra được công bố trên tờ báo "Le Monde" của Pháp vào tháng 1/2018 chỉ ra rằng, tài liệu bí mật của trụ sở chính Liên minh châu Phi (AU) đặt tại Ethiopia mỗi đêm đều được gửi đến Thượng Hải, việc này đã diễn ra liên tục trong 5 năm. Một bản báo cáo mới của viện nghiên cứu chính sách chiến lược Úc (ASPI) được công bố ngày 13/7/2018 tiết lộ rằng, Huawei là nhà cung cấp một số thiết bị hạ tầng kỹ thuật mạng internet cho tòa nhà trụ sở của AU. [7]

Tiến sĩ André Ken Jakobsson thuộc Trung tâm nghiên cứu quân sự của Đại học Copenhagen nói: "Điều đáng lo ngại là đcstq có thể thu được những thông tin vô cùng quan trọng và nhạy cảm, từ đó họ có thể khống chế toàn bộ hệ thống xã hội của chúng tôi. Trong tương lai tất cả mọi thứ đều sẽ được kết nối với mạng 5G. Chúng tôi lo sợ rằng quốc gia cung cấp loại thiết bị này, tq sẽ khống chế mọi hoạt động trên mạng."

Tháng 6/2015, chính phủ liên bang Mỹ bị một hacker tq thâm nhập, lấy đi một lượng lớn thông tin cơ mật, thông tin của hơn 21,5 triệu công dân Mỹ đã bị đánh cắp. Những người bị ảnh hưởng bao gồm 19,7 triệu nhân viên chính phủ, và 1,8 triệu người nhà của các nhân viên chính phủ kể trên. "Điều đáng lo ngại là đcstq có thể thu được những thông tin vô cùng quan trọng và nhạy cảm, từ đó họ có thể khống chế toàn bộ hệ thống xã hội của chúng tôi."

Tháng 11/2018, tập đoàn Marriott International tuyên bố, thông tin cá nhân trong hộ chiếu của 500 triệu khách hàng đã bị hacker tấn công, sự việc này bắt đầu diễn ra từ năm 2014. Ngày 12/12, Bộ trưởng ngoại giao Hoa Kỳ Mike Pompeo xác nhận rằng đó là hành vi của đcstq. Marriott là nhà cung cấp khách sạn lớn nhất cho chính phủ và quân nhân Mỹ.

Theo hồ sơ tòa án ngày 20/7, một nhà nghiên cứu tq bị buộc tội gian lận visa vì che giấu mối quan hệ với quân đội tq (PLA) đang lẩn trốn trong LSQ nước này tại San Francisco được 1 tháng.

Trước đó, FBI đã cảnh báo trong nhiều năm rằng các trường đại học ở Mỹ có nguy cơ bị đánh cắp tài sản trí tuệ từ các nhà nghiên cứu nước ngoài. Gần đây, Mỹ cũng đã thắt chặt các hạn chế đối với thị thực sinh viên.

Ông nhấn mạnh: "Lãnh sự quán đcstq ở Houston đứng sau tất cả hoạt động này và có lịch sử tham gia vào hành vi gây hại cho nước Mỹ". Tháng 11-2019, một nhân viên tq của Tập đoàn năng lượng Phillips 66 (Houston) nhận tội đã ăn cắp thông tin mật về công nghệ pin thế hệ mới của công ty.

Theo ông Anthony Roman – một chuyên gia về an ninh ở New York, những năm gần đây chính phủ tq đã đẩy mạnh hoạt động chiến tranh mạng, thu dụng từ 50.000-100.000 nhân viên dân sự và quân sự cho nỗ lực này.

Những năm gần đây chính phủ tq đã đẩy mạnh hoạt động chiến tranh mạng, thu dụng từ 50.000-100.000 nhân viên dân sự và quân sự cho nỗ lực này. "Nỗ lực (chiến tranh mạng) của tq lớn chưa từng thấy. Hoạt động tình báo và tấn công mạng của họ không đo đếm được. Tất cả hạ tầng chiến lược ở Mỹ đều là mục tiêu", ông Roman nhận xét.
Pompeo: "Chúng ta đang phải đối mặt với con quái vật đcstq"

Các hành vi trộm cắp tài sản trí tuệ của tq gây thiệt hại cho nền kinh tế Mỹ hàng tỷ USD và gây tổn thất hàng ngàn việc làm. Nhiều nhà phân tích nói rằng nếu muốn đánh ngã đcstq thì phải cắt đứt nguồn thu nhập này. Tuy vậy, Bắc Kinh khẳng định không trộm cắp tài sản trí tuệ.

The Wall Street Journal đã đăng về nạn trộm cắp tài sản trí tuệ khi cảnh cáo Mỹ rằng

“Tin tặc tq đang nhắm mục tiêu vào các trường đại học, công ty dược phẩm và các công ty chăm sóc sức khoẻ của Mỹ nhằm đánh cắp tài sản trí tuệ liên quan đến phương pháp điều trị và vắc-xin coronavirus và các cuộc xâm nhập có thể gây nguy hiểm cho tiến trình nghiên cứu y học”.

Theo Washington Post: “tq đánh cắp tài sản trí tuệ và nghiên cứu nhằm củng cố nền kinh tế của họ, và sau đó họ sử dụng lợi ích bất hợp pháp đó làm vũ khí để bịt miệng bất kỳ quốc gia nào dám thách thức các hành động phi pháp của họ.
Phó Giám đốc FBI David Bowdich kết luận: “Đây là kiểu ép buộc kinh tế không phải là điều chúng ta mong đợi từ một nhà lãnh đạo thế giới đáng tin cậy. Đó là những gì chúng tôi thấy từ một băng đảng tội phạm có tổ chức”.

Nguồn tài nguyên mà tc dùng để xâm nhập vào các quốc gia trên thế giới lớn vượt quá sức tưởng tượng của con người, những gì sự thực được vạch trần chỉ là một góc của tảng băng chìm. Các nước trên thế giới đều bắt đầu cảm nhận rõ ràng dã tâm toàn cầu và thủ đoạn tà ác, sức phá hoại “không giới hạn” của đcstq.

Bộ trưởng Ngoại giao Hoa Kỳ Pompeo tại Thư viện Tổng thống Richard Nixon phát biểu hôm nay về chính sách đối ngoại của Hoa Kỳ đối với tq trong những năm tiếp theo.

"tq đã ăn cắp tài sản trí tuệ và bí mật thương mại của chúng ta, làm mất hàng triệu việc làm trên khắp nước Mỹ. tq đã khiến chuỗi cung ứng rời khỏi Hoa Kỳ, và đã sử dụng lao động với cách thức giống hệt như với những nô lệ. tq đã khiến cho các tuyến hàng hải huyết mạch của thế giới trở nên kém an toàn hơn cho thương mại quốc tế. Tổng thống Nixon đã từng nói ông sợ rằng ông đã tạo ra một con quái vật bằng cách giúp cho đcstq hội nhập với thế giới, và chúng ta đang phải đối mặt với con quái vật ấy."

“Điều đáng lo ngại là đcstq có thể thu được những thông tin vô cùng quan trọng và nhạy cảm, từ đó họ có thể khống chế toàn bộ hệ thống xã hội của chúng tôi." (Max Pixel)

Những năm gần đây chính phủ tq đã đẩy mạnh hoạt động chiến tranh mạng, thu dụng từ 50.000-100.000 nhân viên dân sự và quân sự cho nỗ lực này. (Max Pixel)
(Còn tiếp)

***Chú thích**: Theo các nghiên cứu của The Epoch Times*
[1]- Tìm hiểu về đường sắt cao tốc: “Tuyến đường sắt cao tốc Phong Vân” Trường Sa: Nhà xuất bản văn nghệ Hồ Nam, năm 2015), Chương 5 “Đường Sắt cao tốc Trung Quốc đánh bại 3 quốc gia”
[2]- “Chinese Hackers Indicted,” FBI News, 20/12/2018,
[3]- Zach Dorfman, “How Silicon Valley Became a Den of Spies,” Politico, 27/7/2018,
[4]- Lawrence A. Tabak and M. Roy Wilson, “Foreign Influences on Research Integrity,” Presentation at the 117th Meeting of the Advisory Committee to the Director, NIH,
[52]Keith Bradsher, “When Solar Panels Became Job Killers,” The New York Times, 8/4/2017

[5]- "Luật tình báo nước cộng hòa nhân dân Trung Hoa", Mạng nhân dân quốc gia Trung Quốc, 27/6/2017,
[6]- "Statement of John C. Demers before the Committee on the Judiciary United States Senate for a Hearing on China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses," US Senate, 12/12/2018
[7]- Danielle Cave, "The African Union Headquarters Hack and Australia's 5G Network," Australian Strategic Policy Institute
[8]- Đường Minh: "Hacker Trung Quốc ngụy trang website của Pháp Luân Công ở Mỹ kêu gọi Trung Quốc tuân thủ quy tắc quốc tế", http://www.epochtimes.com/gb/13/3/16/n3824225.htm