

*Cường quốc nhờ trộm cắp
Đường Thư*

Những biện pháp này vẫn còn được coi là công khai, nhưng trực tiếp dùng các thủ đoạn phi pháp để đánh cắp công nghệ của phương Tây mới là đòn hiểm của đctq nhằm vượt mặt về công nghệ.

Thủ đoạn trộm công nghệ của tc vượt xa so với phạm vi gián điệp thương mại trước đây, nó sử dụng thủ đoạn “đại dương rộng lớn của chiến tranh nhân dân”, sử dụng tất cả những người có thể sử dụng được, bao gồm gián điệp viên chức, hacker, du học sinh, phóng viên, người dân di cư từ tq đại lục và Đài Loan làm việc trong các công ty phương Tây cho đến những người phương Tây bị dụ dỗ, không ai là nó không lợi dụng để đánh cắp bí mật công nghệ của phương Tây.

Christopher Wray, cục trưởng FBI nói, “Mục tiêu của Trung Quốc là thay thế nước Mỹ trở thành nước lớn siêu cấp đi đầu thế giới, họ đang dùng mọi thủ đoạn phi pháp để thực hiện mục tiêu này”. [2]

Bằng thủ đoạn "chiến tranh nhân dân", đctq cũng tỏ ra cực kỳ lọc lõi khi biến những công dân bình thường trở thành những tên gián điệp, tiếp tay cho sự bành trướng độc tài của chế độ này.

Rất nhiều công ty mới khởi nghiệp ở thung lũng Silicon, Mỹ đều cần vốn. tq không ngần ngại dùng tiền của quốc gia để đầu tư vào các công ty mới khởi nghiệp của Mỹ này, dùng cách này để nắm giữ công nghệ thế hệ mới. Những sản phẩm do các công ty mới khởi nghiệp nghiên cứu phát triển bằng tiền đầu tư của tq bao gồm động cơ tên lửa hàng không vũ trụ, radar của tàu hải quân tự lái, thiết bị màn hình uốn dẻo và máy in sử dụng trong khoang lái của máy bay chiến đấu, v. v...



Ngày 20/12/2018, Bộ Tư pháp Mỹ khởi tố hai công dân tq nằm trong tổ chức hacker “APT 10” có quan hệ mật thiết với chính phủ tq, tổ chức này đã thực hiện hàng loạt

vụ tấn công hacker trên diện rộng, đánh cắp được một lượng thông tin khổng lồ từ hơn 45 tổ chức trong đó có NASA và bộ năng lượng Mỹ, gồm các lĩnh vực chăm sóc sức khỏe, công nghệ sinh học, tài chính, công nghiệp chế tạo, dầu mỏ và khí đốt.

Kathleen Puckett, một nhân viên tình báo Mỹ đã làm công việc chống gián điệp trong thời gian dài ở San Francisco, nói: đcstq “dồn tất cả nỗ lực vào hoạt động gián điệp, và nó đã đạt được mọi thứ một cách miễn phí”. [3]

Chiến tranh tình báo trong thời đại điện tử hoàn toàn khác với hành vi gián điệp đi chụp vài trang tài liệu trước đây. Cái mà đcstq đánh cắp được là cơ sở dữ liệu hoàn chỉnh của một công nghệ nào đó, hơn nữa rất nhiều trường hợp là lấy đi cả người và công nghệ, thêm vào đó cùng với sức mạnh đáng kinh ngạc của công xưởng thế giới mà tq tạo ra được trong mấy chục năm qua, cùng với việc tq đầu tư dài hạn vào nâng cao năng lực nghiên cứu phát triển, đcstq quả thực là có thể đánh cắp mọi thứ để tạo ra một “cường quốc chế tạo”.

Thời đại công nghệ số cho phép đcstq đánh cắp cơ sở dữ liệu hoàn chỉnh của một công nghệ nào đó, cùng với những thế mạnh sẵn có, đcstq quả thực có thể cướp mọi thứ để tạo ra một "cường quốc chế tạo".

Kế hoạch ngàn người tài - biến nhân tài thành gián điệp

Từ khi tq mở cửa đất nước, đã có đến hàng triệu học sinh tq du học ra nước ngoài. chiêu mộ, dùng mức lương cao để mời gọi những nhân tài lợi dụng những nhân tài cao cấp được phương Tây bồi dưỡng này ở hải ngoại về tq làm việc, kêu gọi họ trực tiếp “du nhập” những thông tin kinh tế và những công nghệ tiên tiến do phương Tây đầu tư nghiên cứu phát triển vào tq, giúp nó thực hiện dã tâm thống lĩnh toàn thế giới.

Ông David Stillwell, Trợ lý ngoại trưởng Mỹ phụ trách Đông Á và Thái Bình Dương nói với tờ NYTimes hôm 22/7: “Quân đội đcstq đã gửi sinh viên cả công khai lẫn bí mật tới các trường Đại học Mỹ để nghiên cứu những thứ có thể thúc đẩy lợi thế chiến tranh của họ trong thế giới kinh tế và các lĩnh vực khác”.

Trong hồ sơ giải mật liên quan đến “Kế hoạch nhân tài của tq (kế hoạch ngàn người tài)” vào tháng 9/2015, Cục điều tra liên bang Mỹ đã tổng kết rằng: “Chiêu mộ những người này giúp tq có thể:

- Thu được những nghiên cứu công nghệ và kiến thức chuyên môn mũi nhọn của Mỹ;
- Kiếm lợi từ những nghiên cứu khoa học mà Mỹ đã tiến hành trong nhiều năm, mà những nghiên cứu này lại được đầu tư bởi chính phủ và các doanh nghiệp tư nhân của Mỹ;
- Ảnh hưởng nghiêm trọng đến nền kinh tế Mỹ.

Một báo cáo ngày 13/12/2018 của Viện sức khỏe quốc gia Mỹ (NIH) nhắm vào kế hoạch ngàn người tài của đcstq đã vạch rõ những nhân viên nghiên cứu người nước ngoài này vừa nhận tiền của chính phủ Mỹ, vừa đem những sở hữu trí tuệ của Mỹ chuyển về quốc gia mình, khiến cho những tổ chức học thuật trên toàn nước Mỹ trở thành đối tượng bị thiệt hại. [4]

Số người liên quan đến kế hoạch ngàn người tài của đcstq trên thực tế có thể đã lên đến hàng vạn người và vẫn không dừng lại, gần như đã vơ vét hết những tài năng khoa học kỹ thuật đã từng du học ở Mỹ từ những năm 1980 đến nay. Thực chất đcstq

đang dùng toàn bộ sức mạnh quốc gia để tiến hành cuộc chiến tranh không giới hạn giành giật nhân tài và sở hữu trí tuệ.

Toàn dân trở thành gián điệp

ĐCSQT dùng các quy định pháp luật để trói buộc toàn thể người tỵ vào cuộc chiến không giới hạn này. Theo “Luật tình báo quốc gia”: “Cơ quan tình báo quốc gia có thể yêu cầu các cơ quan, tổ chức và công dân có liên quan giúp đỡ, hợp tác và phối hợp khi cần thiết”. [5]

Điều này có nghĩa là bất cứ công dân tỵ nào cũng có thể bị ĐCSQT cưỡng ép thu thập thông tin tình báo, trở thành gián điệp, cuộc chiến tranh gián điệp này có đã đạt quy mô trước nay chưa từng thấy.

John Demers trợ lý kiểm sát trưởng của Bộ an ninh quốc gia thuộc Bộ tư pháp Mỹ đã nói rằng “kế hoạch phát triển ngành chế tạo quốc gia đến năm 2025” của ĐCSQT bề ngoài chỉ là “chỉ đạo về phát triển công nghệ”, thực chất là chỉ đạo sự đánh cắp. Ông tiết lộ, từ năm 2011 đến năm 2018, trong số những vụ việc gián điệp kinh tế liên quan đến hoặc có lợi cho quốc gia nào đó do bộ này điều tra, có hơn 90% vụ việc có liên quan đến tỵ; và hơn 2/3 số vụ việc đánh cắp bí mật thương mại được bộ này xử lý cũng có liên quan đến tỵ [6]

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 nguy 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>

Bằng thủ đoạn "chiến tranh nhân dân", ĐCSQT cũng tỏ ra cực kỳ lọc lõi khi biến những công dân bình thường trở thành những tên gián điệp, tiếp tay cho sự bành trướng độc tài của chế độ này. (Wikimedia Commons)

Quý Siêu Quân (trái) - một gián điệp thế hệ mới của ĐCSQT dưới mào "du học sinh".

