KHÔNG NƠI ẨN NẤP

Edward Snowden,
NSA và nhà nước giám sát

Glenn Greenwald

Chương 3:
Thu thập tất cả

&

Chương 4:
Tác hại của sự giám sát

Dịch sang tiếng Việt: Lê Trung Nghĩa, letrungnghia.foss@gmail.com
Dịch xong: 21/07/2014
Bản gốc tiếng Anh: https://www.dropbox.com/s/91814hqjm2dczuq/NoPlaceToHide4Fr33.pdf

---

NO PLACE TO HIDE

Edward Snowden,
NSA & Surveillance State

Glenn Greenwald

Chapter 3:
Collect It All

&

Chapter 4:
The harm of surveillance

Mục lục

VỀ TÁC GIẢ

Glenn Greenwald là tác giả của vài cuốn sách bán chạy nhất nước Mỹ, bao gồm Thế nào là Luật Yêu nước? (How Would A Patriot Act) và Di sản Bi thương (A Tragic Legacy). Được tờ Atlantic đưa lên như một trong 25 nhà bình luận chính trị có ảnh hưởng nhất, Greenwald là cựu luật sư về luật hiến pháp và các quyền dân sự. Ông từng phụ trách một chuyên mục cho tờ Guardian và các tác phẩm của ông đã xuất hiện trên vô số báo và tạp chí tin tức chính trị, bao gồm cả tờ New York Times và Los Angeles Times. Vào tháng 02/2014 ông đã khởi xướng một tổ chức phương tiện mới, Fist Look Media.

Hãy theo ông trên Twitter tại @ggreenwald.

CŨNG CỦA GLENN GREENWALD

- Luật Yêu nước là thế nào?
- Di sản bi thương
- Những kẻ đạo đức giả lớn người Mỹ
- Với tự do và công lý cho một số

Cuốn sách này dành cho tất cả những ai đã tìm cách rọi ánh sáng vào các hệ thống giám sát ồ ạt bí mật của chính phủ Mỹ, đặc biệt cho những người thổi còi dũng cảm đã mạo hiểm sự tự do của họ để làm thế.

Chính phủ Mỹ đã làm hoàn hảo một khả năng công nghệ cho phép chúng ta theo dõi các thông điệp đi qua không trung... Khả năng đó bất kỳ lúc nào cũng có thể quay lại với những người Mỹ, và không người Mỹ nào có thể có được bất kỳ tính riêng tư nào được để lại, thứ đó là khả năng theo dõi mọi điều - các cuộc hội thoại qua điện thoại, không là vấn đề gì. Có lẽ không còn có nơi nào để ẩn nấp nữa.

- Thượng nghị sỹ Frank Church, Chủ tịch, Ủy ban Bầu chọn Thượng viện về Nghiên cứu các Hoạt động của Chính phủ với Lưu ý về các Hoạt động Tình báo, 1975

GIỚI THIỆU

Vào mùa thu năm 2005, không có nhiều kỳ vọng lớn lao trên đường đi, tôi đã quyết định tạo ra một blog chính trị. Tôi đã có một ít ý tưởng khi đó về việc liệu quyết định này cuối cùng có thể thay đổi cuộc sống của tôi được bao nhiêu. Động lực cơ bản của tôi từng là tôi đã ngày càng trở nên bị cảnh báo từ các lý thuyết của những người cực đoan và cấp tiến rằng việc viết về các vấn đề như vậy có thể cho phép tôi thực hiện ảnh hưởng rộng lớn hơn mà tôi có thể trong sự nghiệp sau này của tôi như một luật sư theo hiến pháp và các quyền dân sự.

Chỉ 7 tuần sau đó tôi đã bắt đầu viết blog, khi tờ *New York Times* đã làm xôn xao dư luận: vào năm 2001, nó đã nêu, chính quyền Bush đã bí mật ra lệnh cho Cơ quan An ninh Quốc gia - NSA (National Security Agency) để nghe lén các giao tiếp truyền thông điện tử của những người Mỹ mà không có lệnh cho phép được luật chống tội phạm phù hợp yêu cầu. Vào thời điểm mà điều đó bị tiết lộ, việc nghe lén không có lệnh cho phép này đã và đang tiến hành được 4 năm rồi và đã nhằm vào ít nhất vài ngàn người Mỹ.

Chủ đề đó từng là một sự hội tụ tuyệt vời đối với niềm đam mê của tôi và sự tinh thông của tôi. Chính phủ đã cố chứng minh chương trình bí mật của NSA bằng việc viện tới chính xác dạng lý thuyết cực đoan về sức mạnh thực thi mà đã tạo động lực cho tôi để bắt đầu viết: lưu ý rằng mối đe dọa của chủ nghĩa khủng bố đã trao cho tổng thống hầu như quyền không hạn chế để làm bất kỳ điều gì để "giữ cho dân tộc được an toàn", bao gồm cả quyền để vi phạm luật. Cuộc tranh luận tiếp theo đã kéo theo những câu hỏi phức tạp về luật theo hiến pháp và sự giải nghĩa theo luật định, mà cơ sở pháp lý của tôi đã trao cho tôi cơ hội phù hợp để đề cập tới.

Tôi đã bỏ ra 2 năm tiếp sau đề cập tới từng khía cạnh của vụ lùm xùm nghe lén không có lệnh cho phép của NSA, trên blog của tôi và trong một cuốn sách bán chạy nhất năm 2006. Quan điểm của tôi từng thẳng thắn: bằng việc ra lệnh nghe lén bất hợp pháp, tổng thống đã phạm tội và nên bị truy cứu trách nhiệm vì chúng. Trong không khí chính trị hiếu chiến và ngột ngạt ngày càng gia tăng ở Mỹ, điều này đã chứng minh là một lập trường gây tranh cãi mạnh mẽ.

Chính nền tảng cơ sở này đã nhắc nhở Edward Snowden, vài năm sau, chọn tôi như là người liên hệ đầu tiên của anh ta cho việc tiết lộ những việc làm sai trái của NSA trong một phạm vi thậm chí còn ồ ạt hơn. Anh ta đã nói anh ta đã tin tưởng là tôi có thể được tính tới để hiểu được những mối nguy hiểm của sự giám sát ồ ạt và bí mật nhà nước cực đoan, và không lùi bước khi đối mặt với áp lực từ chính phủ và nhiều đồng minh của chính phủ trong giới truyền thông và cả ở những nơi khác nữa.

Số lượng phi thường các tài liệu tuyệt mật mà Snowden đã chuyển cho tôi, cùng với bi kịch cao độ xung quanh bản thân Snowden, đã tạo ra sự thú vị chưa từng thấy khắp thế giới trong mối đe dọa giám sát điện tử ồ ạt và giá trị của tính riêng tư trong kỷ nguyên số. Nhưng những vấn đề nằm bên dưới đã và đang mưng mủ từ nhiều năm, phần lớn trong bóng tối.

Chắc chắn, sẽ có nhiều khía cạnh độc nhất vô nhị đối với sự tranh cãi hiện hành về NSA. Công nghệ bây giờ đã cho phép một dạng giám sát tràn ngập khắp mọi nơi mà trước đó chỉ có trong lãnh địa của những nhà văn viết chuyện khoa học viễn tưởng giàu trí tưởng tượng nhất. Hơn nữa, sự

sùng kính an ninh trên hết của những người Mỹ sau sự kiện ngày 11/09 đã tạo ra một môi trường đặc biệt thuận lợi để lạm dụng sức mạnh. Và nhờ sự dũng cảm của Snowden và sự lơi lỏng tương đối của việc sao chép các thông tin số, chúng ta có một cái nhìn trực tiếp không gì bằng vào các chi tiết về cách mà hệ thống giám sát đó thực tế vận hành.

Hơn nữa, trong nhiều lưu ý các vấn đề mà câu chuyện của NSA đã làm dấy lên được cộng hưởng với vô số câu chuyện từ quá khứ, kéo ngược lại xuyên khắp các thế kỷ. Quả thực, phản đối về sự can thiệp của chính phủ đối với tính riêng tư từng là một yếu tố chính trong sự thiết lập bản thân nước Mỹ, như những người thực dân Mỹ từng phản đối luật cho phép các quan chức Anh lục soát bất cứ lúc nào bất kỳ ngôi nhà nào mà họ muốn. Điều đó từng là hợp pháp, những người thực dân đã đồng ý, cho nhà nước có được các lệnh cho phép đặc biệt, có chủ đích để lục soát các cá nhân khi có bằng chứng để thiết lập lý do có thể đối với việc làm sai trái của họ. Nhưng các lệnh cho phép chung chung - vốn dĩ là bất hợp pháp.

Sửa đổi bổ sung số 4 đã lưu giữ ý tưởng này trong luật Mỹ. Ngôn ngữ của nó là rõ ràng và cô đọng: "Quyền của mọi người có an ninh đối với thân thể, nhà cửa, giấy tờ của họ, và kết quả, chống lại những lục soát và bắt giữ không có lý do, sẽ không bị vi phạm, và không lệnh cho phép nào sẽ ban hành, mà dựa vào lý do có thể, được lời tuyên thệ hoặc khẳng định hỗ trợ, và đặc biệt mô tả nơi sẽ bị lục soát, và những người hoặc đồ vật bị bắt giữ". Trên tất cả, đã từng có ý định bãi bỏ vĩnh viễn ở nước Mỹ sức mạnh của chính phủ để bắt các công dân của mình chịu sự giám sát suy rộng, không có tình nghi.

Sự xung đột về giám sát trong thế kỷ 18 đã tập trung vào lục soát nhà cửa, nhưng khi công nghệ đã tiến hóa, thì sự giám sát đã tiến hóa cùng với nó. Vào giữa thế kỷ 19, khi sự lan tràn của đường sắt đã bắt đầu cho phép phân phối thư rẻ và nhanh, thì việc mở thư lén lút của chính phủ Anh đã gây ra một vụ lùm xùm chính ở nước Anh. Vào các thập kỷ đầu của thế kỷ 20, Cục Điều tra của Mỹ (US Bureau of Investigation) - tiền thân của Cục Điều tra Liên bang - FBI (Federal Bureau of Investigation) ngày nay - từng sử dụng nghe lén, cùng với việc theo dõi thư và những người cung cấp tin, để kiểm soát chặt chẽ những người chống lại các chính sách của chính phủ Mỹ.

Bất kể kỹ thuật đặc biệt gì có liên quan, sự giám sát ồ ạt theo lịch sử đã có vài thuộc tính bất biến. Ban đầu, nó luôn là những người bất đồng chính kiến và được cách li ra khỏi sự phát triển xã hội của nước đó, những người mang gánh nặng của sự giám sát, dẫn dắt những người mà ủng hộ chính phủ hoặc chỉ là thờ ơ tin tưởng sai lầm là họ được miễn trừ. Và lịch sử chỉ ra rằng chỉ là sự tồn tại của một bộ máy giám sát ồ ạt, bất kể cách mà nó được sử dụng, bản thân nó là đủ để bóp nghẹt sự bất đồng chính kiến. Toàn thể công dân mà nhận thức được việc luôn bị theo dõi sẽ nhanh chóng trở thành toàn thể công dân phục tùng mệnh lệnh và sợ hãi.

Cuộc điều tra giữa những năm 1970 của Frank Church trong việc gián điệp của FBI đã thấy một cách sốc rằng cơ quan đó đã gắn nhãn cho một nửa triệu công dân Mỹ như là "có tính lật đổ" tiềm năng, thường xuyên gián điệp mọi người thuần túy chỉ dựa vào niềm tin chính trị của họ. (Danh sách các mục tiêu của FBI đã trải từ Martin Luther King cho tới John Lennon, từ phong trào tự do của phụ nữ cho tới Xã hội chống cộng sản của John Birch). Nhưng bệnh dịch lạm dụng giám sát là

duy nhất khắc nghiệt đối với lịch sử của những người Mỹ. Ngược lại, giám sát ồ ạt là sự cám dỗ vạn năng đối với bất kỳ sức mạnh vô lương tâm nào. Và trong từng trường hợp, động lực là y hệt nhau: đàn áp bất đồng chính kiến và áp đặt tuân thủ.

Giám sát vì thế hợp nhất các chính phủ của các tín điều chính trị khác nhau đáng kể. Vào đầu thế kỷ 20, các đế quốc Anh và Pháp đã tạo ra các cục giám sát đặc biệt để làm việc với các mối đe dọa của các phong trào chống thực dân. Sau Chiến tranh Thế giới 2, Bộ An ninh Nhà nước Đông Đức, nổi tiếng được biết như là Stasi, đã trở thành biểu tượng với sự thâm nhập trái phép của chính phủ vào cuộc sống cá nhân. Và gần đây hơn, khi các cuộc chống đối của nhân dân trong Mùa xuân Ả rập đã thách thức tiếm quyền của các nhà độc tài, thì các chế độ ở Syria, Ai cập, và Libya tất cả đều tìm cách gián điệp bằng việc sử dụng Internet đối những người bất đồng chính kiến trong nước.

Các điều tra nghiên cứu của *Bloomberg News* và *Tạp chí Phố Uôn* (*Wall Street Journal*) đã chỉ ra rằng khi các chế độ độc tài đó bị những người phản đối lấn át, họ theo nghĩa đen đã đi mua sắm các công cụ giám sát từ các công ty công nghệ phương Tây. Chế độ Assad của Syria đã cậy nhờ tới các nhân viên từ công ty giám sát Area SpA của Ý, những người được nói rằng những người Syria "cấp bách cần theo dõi mọi người". Tại Ai cập, cảnh sát bí mật của Mubarak đã mua các công cụ để thâm nhập mã hóa Skype và nghe lén các cuộc gọi của các nhà hoạt động xã hội. Và ở Libya, như Tạp chí Phố Uôn đã nêu, các nhà báo và những người nổi dậy đã vào được một trung tâm giám sát của chính phủ trong năm 2011 và đã thấy "một bức tường các thiết bị màu đen có kích thước bằng chiếc tủ lạnh" từ công ty giám sát của Pháp Amesys. Thiết bị "đã kiểm tra giao thông Internet" của nhà cung cấp dịch vụ Internet chính của Libya, "mở các thư điện tử, đoán các mật khẩu, rình mò các cuộc chat trực tuyến và lập bản đồ các kết nối giữa những người bị tình nghi khác nhau".

Khả năng nghe lén các giao tiếp truyền thông của mọi người trao sức mạnh bao la cho những người tiến hành nó. Và trừ phi sức mạnh như vậy nằm trong sự kiểm tra với sự hiểu thấu và trách nhiệm giải trình mãnh liệt, nó hầu như chắc chắn sẽ bị lạm dụng. Kỳ vọng việc chính phủ Mỹ vận hành bộ máy giám sát ồ ạt trong sự bí mật hoàn toàn mà không có con mồi nào rơi vào sự cám dỗ của nó là ngược với mọi ví dụ lịch sử và tất cả các bằng chứng sẵn có về bản chất tự nhiên của con người.

Quả thực, thậm chí trước cả những tiết lộ của Snowden, đã là rõ ràng rồi rằng việc đối xử với nước Mỹ vì bất kỳ lý do gì như một ngoại lệ về vấn đề giám sát là một quan điểm ngây thơ cao độ. Vào năm 2006, trong một cuộc điều trần của quốc hội mang tên "Internet ở Trung Quốc: Một công cụ cho Tự do hay Đàn áp?", các diễn giả đã lần lượt lên án các công ty công nghệ Mỹ vì giúp Trung Quốc đàn áp bất đồng chính kiến trên Internet. Christopher Smith (R-NJ), nghị sỹ quốc hội chủ trì cuộc điều trần, đã so sánh tập đoàn Yahoo! với cảnh sát mật của Trung Quốc để trao Anne Frank cho bọn Phát xít. Đó từng là một bài diễn thuyết trước đám đông, một trình diễn điển hình khi các quan chức Mỹ nói về một chế độ không phù hợp với nước Mỹ.

Nhưng thậm chí những người tham dự của quốc hội cũng không thể giúp lưu ý được rằng cuộc điều trần ngẫu nhiên đã diễn ra chỉ 2 tháng sau khi tờ *New York Times* đã tiết lộ việc nghe lén khổng lồ ở trong nước mà không có lệnh cho phép được chính quyền Bush triển khai. Cùng với những tiết lộ đó, việc vạch mặt các nước khác vì triển khai giám sát trong nước của riêng họ xem ra khá là rỗng

tuếch. Đại diện Brad Sherman (D-CA), nói sau Đại diện Smith, đã lưu ý rằng các công ty công nghệ đang được nói để phản kháng lại chế độ của Trung Quốc cũng nên thận trọng lưu ý chính phủ của riêng họ. "Nếu khác", ông đã cảnh báo trước, "trong khi những người ở Trung Quốc có lẽ thấy tính riêng tư của họ bị vi phạm theo những cách thức tàn ác nhất, thì chúng ta ở đây ở nước Mỹ có lẽ cũng thấy rằng có lẽ một số tổng thống trong tương lai sẽ khẳng định những giải thích rất rộng đó của Hiến pháp là được đọc thư điện tử của chúng ta, và tôi thích nó không xảy ra hơn khi không có lệnh của một tòa án".

Vài thập kỷ qua, nỗi sợ hãi chủ nghĩa khủng bố - được đốt lên nhờ những thổi phồng kiên định trước sau như một về mối đe dọa thực sự - đã được các nhà lãnh đạo nước Mỹ khai thác để chứng minh cho một dải rộng lớn các chính sách cực đoan. Điều đó đã dẫn tới các cuộc chiến tranh xâm lược, một chế độ tra tấn khắp thế giới, và sự cầm tù (và thậm chí ám sát) cả những người của các nước khác và các công dân Mỹ mà không có bất kỳ sự kết án nào. Nhưng hệ thống giám sát không cần nghi ngờ, bí mật và ở đâu cũng có mà nó đã sinh sôi nảy nở có thể rất tốt hóa ra là di sản dài lâu nhất của nó. Điều này là như vậy vì, bất chấp tất cả các tương đồng lịch sử, cũng có một kích cỡ mới thực sự cho vụ lùm xùm giám sát hiện hành của NSA: bây giờ vai trò được Internet đóng trong cuộc sống hàng ngày.

Đặc biệt đối với thế hệ trẻ hơn, thì Internet không chỉ là thứ gì đó đứng một mình, một miền cách li nơi mà một ít chức năng của cuộc sống được triển khai. Nó không chỉ là cái bưu điện của chúng ta và điện thoại của chúng ta. Thay vào đó, nó là tâm chấn thế giới của chúng ta, là nơi mà hầu hết mọi điều được thực hiện. Đó là nơi mà bạn bè được hình thành, là nơi mà các cuốn sách và các bộ phim sẽ được chọn, là nơi mà các hoạt động chính trị xã hội sẽ được tổ chức, là nơi mà hầu hết các dữ liệu riêng tư được tạo ra và lưu trữ. Nó là nơi mà chúng ta phát triển và thể hiện cá tính và sự tự giác của chúng ta.

Biến mạng đó thành một hệ thống giám sát ồ ạt có những tác động không giống như những tác động của bất kỳ chương trình giám sát nhà nước trước đó nào. Tất cả các hệ thống giám điệp trước kia nhất thiết từng bị hạn chế hơn và có khả năng tránh được. Để cho phép giám sát nắm được gốc rễ trên Internet có thể có nghĩa là phải chịu hầu như tất cả các dạng tương tác của con người, việc lên kế hoạch, và thậm chí tự nghĩ về sự kiểm tra của nhà nước một cách toàn diện.

Từ thời điểm mà nó lần đầu bắt đầu được sử dụng rộng rãi, Internet đã được nhiều người xem như là việc chiếm hữu một tiềm năng to lớn khác thường: khả năng giải phóng hàng trăm triệu người bằng việc dân chủ hóa đàm luận chính trị và tận dụng sân chơi bình đẳng giữa có quyền và không có quyền. Tự do Internet - khả năng để sử dụng mạng mà không có các ràng buộc, kiểm soát xã hội hoặc nhà nước, và nỗi sợ hãi tràn lan - là trọng tâm để hoàn thành lời hứa đó. Việc biến Internet thành một hệ thống giám sát vì thế lấy đi tiềm năng cốt lõi của nó. Tệ hơn, điều đó biến Internet thành một công cụ đàn áp, đe dọa tạo ra vũ khí thâm nhập của nhà nước đàn áp và cực đoan nhất mà lịch sử loài người từng thấy.

Đó là những gì mà các tiết lộ của Snowden là quá gây choáng váng và quá quan trọng sống còn. Bằng việc dám tiết lộ các khả năng giám sát đáng kinh ngạc của NSA và thậm chí những tham vọng

gây kinh ngạc nhất của nó, anh ta đã làm rõ, với những tiết lộ đó, rằng chúng ta hãy đứng lên ở một giao lộ lịch sử. Kỷ nguyên số sẽ dẫn dắt tới sự giải phóng cá nhân và các quyền tự do chính trị mà Internet là độc nhất có khả năng dẫn dắt hay không? Hay nó sẽ mang lại một hệ thống giám sát và kiểm soát có mặt ở khắp mọi nơi, vượt ra khỏi những giấc mơ thậm chí của những tên bạo chúa lớn nhất trong quá khứ? Ngay bây giờ, cả 2 con đường đó đều có thể. Các hành động của chúng ta sẽ xác định chúng ta sẽ kết thúc ở đâu.

Chương 3. Thu thập tất cả

Kho lưu trữ các tài liệu mà Edward Snowden đã sưu tập đã gây choáng váng cả về kích cỡ lẫn phạm vi. Thậm chí như ai đó đã trải qua nhiều năm viết về các mối nguy hiểm của giám sát bí mật Mỹ, tôi thấy sự mênh mông khổng lồ của hệ thống gián điệp thật sự gây sốc, tất cả còn hơn thế vì nó rõ ràng từng được triển khai hầu như không có trách nhiệm, không có sự minh bạch, và không có giới hạn.

Hàng ngàn chương trình giám sát riêng rẽ được kho dữ liệu mô tả từng chưa bao giờ được những người đã triển khai chúng có ý định để trở thành tri thức công khai cả. Nhiều chương trình đã nhằm vào dân chúng Mỹ, và hàng tá các nước trên khắp thế giới - bao gồm cả các nền dân chủ thường được coi như là đồng minh của Mỹ, như Pháp, Brazil, Ấn Độ, và Đức - cũng từng là các mục tiêu của sự giám sát ồ ạt bất phân biệt đó.

Kho lưu trữ của Snowden đã được tổ chức tao nhã, nhưng kích cỡ và sự phức tạp của nó làm cho nó cực kỳ khó xử lý. Hàng chục ngàn tài liệu của NSA trong đó hầu như đã được từng đơn vị và đơn vị con trực thuộc bên trong cơ quan rộng lớn này tạo ra, và nó cũng bao gồm cả một vài tệp từ các cơ quan tình báo đồng minh nước ngoài gần gũi. Các tài liệu là gần đây một cách ngạc nhiên: hầu hết từ 2011 và 2012, và nhiều tài liệu từ 2013. Một số thậm chí đề ngày từ tháng 3 và 4 năm đó [2013], chỉ vài tháng trước khi chúng tôi đã gặp được Snowden ở Hong Kong.

Đại đa số các tệp trong kho lưu trữ đó đã được chỉ định là "tuyệt mật". Hầu hết chúng đã được đánh dấu là "FVEY", nghĩa là chúng đã được phê chuẩn để phân phối chỉ cho 4 đồng minh giám sát gần nhất của NSA, liên minh "5 cặp mắt" nói tiếng Anh bao gồm Anh, Canada, Úc và New Zealand. Các tài liệu khác từng có ý chỉ cho các cặp mắt của Mỹ, được đánh dấu là "NOFORN" nghĩa là "không phân phối ra nước ngoài". Các tài liệu nhất định, như lệnh tòa án FISA cho phép thu thập các cuộc ghi điện thoại và chỉ thị của tổng thống Obama để chuẩn bị các tác chiến tấn công không gian mạng, đã nằm trong số các bí mật được giữ chặt chẽ nhất của chính phủ Mỹ.

Việc giải mã kho lưu trữ và ngôn ngữ của NSA có liên quan tới nỗ lực học tập lớn. Cơ quan này giao tiếp với bản thân nó và với các đối tác của nó theo một ngôn ngữ với phong cách đặc thù của riêng nó, một thứ tiếng lóng vừa quan liêu vừa tật nguyền, vâng nhiều lúc khoác lác và thậm chí quái gở. Hầu hết các tài liệu còn đầy rẫy kỹ thuật, đầy rẫy các từ đồng nghĩa và các tên mã ghê gớm, và đôi lúc đòi hỏi rằng các tài liệu khác phải được đọc trước khi chúng có thể được hiểu.

Nhưng Snowden đã biết trước được vấn đề, đưa ra các chú giải các từ đồng nghĩa cho các khái niệm đặc thù. Hơn nữa, một số tài liệu đã không thể hiểu được trong lần đọc thứ nhất, thứ 2, hoặc thậm chí thứ 3. Tầm quan trọng của chúng đã nổi lên chỉ sau khi tôi đã đặt cùng với các phần khác của các tài liệu khác và tư vấn với một số chuyên gia lỗi lạc nhất thế giới về giám sát, mật mã, đột nhập, lịch sử NSA, và khung pháp lý điều chỉnh việc gián điệp của người Mỹ.

Tổng hợp các khó khăn thực tế là hàng núi các tài liệu thường được tổ chức không theo chủ đề mà theo nhánh của cơ quan đó, nơi mà chúng được tạo ra, và những tiết lộ kịch tính đã được trộn vào với số lượng lớn các tư liệu kỹ thuật cao hoặc sáo rỗng. Dù tờ *Guardian* đã sáng chế ra một chương trình để tìm kiếm qua các tệp bằng từ khóa như một trợ thủ đắc lực, thì chương trình đó còn xa mới

là tuyệt hảo. Quá trình phân loại kho lưu trữ từng là chậm và cẩn trọng, và nhiều tháng sau khi chúng tôi lần đầu tiên nhận được các tài liệu, một số khái niệm và chương trình vẫn còn đòi hỏi việc báo cáo tiếp trước khi chúng có thể được tiết lộ một cách an toàn và mạch lạc.

Bất chấp các vấn đề như vậy, các tài liệu của Snowden hiển nhiên đã đặt ra trần trụi một biển tinh vi phức tạp sự giám sát nhằm vào những người Mỹ (những người rõ ràng nằm ngoài nhiệm vụ của NSA) và tương tự nhằm vào những người không phải là người Mỹ. Kho lưu trữ đã tiết lộ các phương tiện kỹ thuật được sử dụng để can thiệp vào các giao tiếp truyền thông: việc nghe lén của NSA đối với các máy chủ Internet, các vệ tinh, các cáp quang ngầm dưới biển, các hệ thống điện thoại nội địa và nước ngoài, và các máy tính cá nhân. Nó đã nhận diện các cá nhân bị ngắm đích cho các dạng gián điệp cực kỳ tràn lan, một danh sách trải từ những tên được cho là khủng bố và các nghi phạm tội phạm cho tới các lãnh đạo được bầu một cách dân chủ của các quốc gia đồng minh và thậm chí cả các công dân Mỹ bình thường. Và nó đã rọi ánh sáng vào toàn bộ các chiến lược và mục tiêu của NSA.

Snowden đã đặt các tài liệu cốt tử, bao quát ở phía trước kho lưu trữ, đánh dấu chúng như là đặc biệt quan trọng. Các tệp đó đã tiết lộ tầm với cực kỳ của cơ quan này, cũng như sự lừa dối và thậm chí sự phạm tội của nó. Chương trình NGƯỜI CUNG CẤP TIN KHÔNG GIỚI HẠN (BOUNDLESS INFORMANT) từng là một trong những tiết lộ đầu tiên như vậy, chỉ ra rằng NSA tính tới tất cả các cuộc gọi điện thoại và các thư điện tử được thu thập hàng ngày từ khắp thế giới với độ chính xác toán học. Snowden đã đặt các tệp đó nổi bật tới mức không chỉ vì chúng đã lượng hóa được số lượng các cuộc gọi và các thư điện tử được NSA thu thập và lưu trữ - theo nghĩa đen tới hàng tỷ cuộc mỗi ngày - mà còn vì chúng đã chứng minh rằng lãnh đạo Keith Alexander và các quan chức khác của NSA đã lừa dối Quốc hội. Lặp đi lặp lại, các quan chức của NSA đã nói rằng họ từng không có khả năng cung cấp các con số cụ thể - chính xác các dữ liệu mà BOUNDLESS INFORMANT từng được xây dựng để thu thập.

Ví dụ, trong giai đoạn một tháng kể từ 08/03/2013, một slide của BOUNDLESS INFORMANT đã chỉ ra rằng chỉ một đơn vị của NSA, Tác chiến Truy cập Toàn cầu (Global Access Operations), đã thu thập các dữ liệu của hơn 3 tỷ cuộc gọi điện thoại và thư điện tử mà đã đi qua hệ thống viễn thông Mỹ. ("DNR", hoặc "Thừa nhận Số Quay số" (Dialed Number Recognition), tham chiếu tới các cuộc gọi điện thoại; "DNI" hoặc "Tình báo Mạng Số" (Digital Network Intelligence), tham chiếu tới các giao tiếp truyền thông dựa vào Internet như các thư điện tử). Điều đó đã vượt qua sự thu thập từ các hệ thống từ từng nước như Nga, Mexico, và hầu như tất cả các nước châu Âu, và tương đương với sự thu thập dữ liệu từ Trung Quốc.

Tổng thể, chỉ trong 30 ngày, đơn vị đó đã thu thập dữ liệu hơn 97 tỷ thư điện tử và 124 tỷ cuộc gọi điện thoại từ khắp thế giới. Một tài liệu khác của BOUNDLESS INFORMANT đã chi tiết các dữ liệu quốc tế được thu thập trong giai đoạn chỉ 30 ngày từ Đức (500 triệu), Brazil (2.3 tỷ), và Ấn Độ (13.5 tỷ). Và còn các tệp khác đã chỉ ra sự thu thập siêu dữ liệu kết hợp với các chính phủ của Pháp (70 triệu), Tây Ban Nha (60 triệu), Ý (47 triệu), Hà Lan (1.8 triệu), Nauy (33 triệu) và Đan Mạch (23 triệu).

Bất chấp trọng tâm được xác định theo qui định pháp luật của NSA vào "tình báo nước ngoài", các tài liệu đã khẳng định rằng dân chúng Mỹ từng là một đích ngắm quan trọng ngang bằng cho sự giám sát bí mật. Không điều gì được thực hiện mà rõ ràng hơn bằng lệnh tuyệt mật ngày 25/04/2013 từ tòa án FISA khi thuyết phục Verizon chuyển cho NSA tất cả các thông tin về các cuộc gọi điện thoại các khách hàng Mỹ của hãng, "các siêu dữ liệu điện thoại". Được đánh dấu là "NOFORN", ngôn ngữ của lệnh đó từng rõ ràng một cách tuyệt đối:

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

Chương trình đồ sộ thu thập điện thoại này từng là một trong những phát hiện quan trọng nhất trong một kho lưu trữ tràn ngập với tất cả các dạng chương trình giám sát giấu giếm - từ PRISM phạm vi rộng (có liên quan tới thu thập dữ liệu trực tiếp từ các máy chủ của các công ty Internet lớn nhất thế giới) và DỰ ÁN BULLRUN, một nỗ lực chung giữa NSA và đối tác nước Anh của nó, Sở Chỉ huy Truyền thông của Chính phủ - GCHQ (Government Communications Headquarters), để đánh bại hầu hết các dạng mã hóa thông thường được sử dụng để bảo vệ các giao dịch trực tuyến, tới các doanh nghiệp mức độ nhỏ hơn với những cái tên mà phản ánh được tinh thần khinh thường và khoác lác về sự siêu việt đằng sau họ: CON HƯƠU CAO CỔ ÍCH KỶ (EGOTISTICAL GIRAFFE), nó nhằm vào trình duyệt Tor, phương tiện để cho phép sự nặc danh trong duyệt trực tuyến; MUSCULAR, phương tiện để đột nhập vào các mạng riêng của Google và Yahoo!; và OLYMPIA, chương trình của Canada để giám sát Bộ Mỏ và Năng lượng của Brazil.

Một vài sự giám sát bề ngoài chuyên tâm vào các nghi phạm khủng bố. Nhưng số lượng lớn các chương trình rõ ràng hiển nhiên không có gì làm với an ninh quốc gia cả. Các tài liệu để lại sự không nghi ngờ rằng NSA từng có liên quan ngang bằng trong gián điệp kinh tế, gián điệp ngoại giao, và giám sát không nghi ngờ gì nhằm vào toàn bộ dân chúng.

Tính tổng số, kho lưu trữ của Snowden đã dẫn tới một kết luận tuyệt đối đơn giản: chính phủ Mỹ đã xây dựng một hệ thống mà nó có mục tiêu loại bỏ hoàn toàn tính riêng tư điện tử trên toàn cầu. Thoát ra khỏi sự khoác lác, điều theo nghĩa đen, rõ ràng đã nêu lên mục tiêu của nhà nước giám sát: để thu thập, lưu trữ, theo dõi, và phân tích tất cả các giao tiếp điện tử của tất cả mọi người khắp thế giới. Cơ quan này chuyên tâm vào một nhiệm vụ xuyên suốt: để ngăn chặn lát mỏng nhất của giao tiếp điện tử khỏi việc tránh được sự chộp lấy một cách có hệ thống của nó.

Mệnh lệnh tự đặt ra này đòi hỏi việc mở rộng bất tận sự vươn tới của NSA. Mỗi ngày, NSA làm việc để nhận diện các giao tiếp điện tử mà không đang được thu thập và lưu trữ và sau đó phát triển các công nghệ và phương pháp mới để sửa cho có hiệu quả. Cơ quan này tự coi bản thân mình như là cần thiết không bào chữa đặc biệt để thu thập bất kỳ giao tiếp điện tử đặc biệt nào, không bất kỳ nền tảng nào cho việc coi các mục tiêu của nó có sự nghi ngờ. Những gì NSA gọi là "SIGINT" - tất cả tình báo dấu hiệu - là mục tiêu của nó. Và chỉ là thực tế rằng việc nó có khả năng thu thập các giao tiếp đó đã trở thành điều căn bản để làm thế.

***

Đối với nhánh quân sự của Lầu 5 góc, thì NSA là cơ quan tình báo lớn nhất thế giới, với đa số công việc giám sát của nó được tiến hành thông qua liên minh 5 cặp mắt. Cho tới mùa xuân năm 2014, khi sự tranh cãi về các câu chuyện của Snowden đã ngày càng trở nên căng thẳng, cơ quan này từng được vị tướng 4 sao Keith B. Alexander lãnh đạo, người đã trông nom nó cả 9 năm trước đó, hung hăng gia tăng kích cỡ và ảnh hưởng của NSA trong nhiệm kỳ của ông ta. Trong quá trình đó, Alexander đã trở thành những gì được nhà báo James Bamford đã mô tả như là "lãnh đạo tình báo mạnh nhất trong lịch sử quốc gia".

NSA "từng là con vật kếch xù về dữ liệu rồi khi Alexander lên nắm quyền", nhà báo của tờ *Chính sách Đối ngoại* (*Foreign Policy*) Shane Harris đã lưu ý, "nhưng dưới sự chăm sóc của ông ta, thì bề rộng, phạm vi, và tham vọng về nhiệm vụ của nó đã mở rộng vượt ra khỏi bất kỳ điều gì những người tiền nhiệm của ông ta từng dự liệu". Chưa bao giờ trước đó có "một cơ quan chính phủ Mỹ từng có khả năng, như một nhà chức trách về pháp lý, để thu thập và lưu trữ quá nhiều thông tin điện tử như thế". Một cựu quan chức hành chính từng làm việc với lãnh đạo NSA đã nói cho Harris rằng "chiến lược của Alexander" từng rõ ràng: "Tôi cần có tất cả các dữ liệu". Và, Harris đã bổ sung, "Ông ta muốn bám vào nó càng lâu có thể càng tốt".

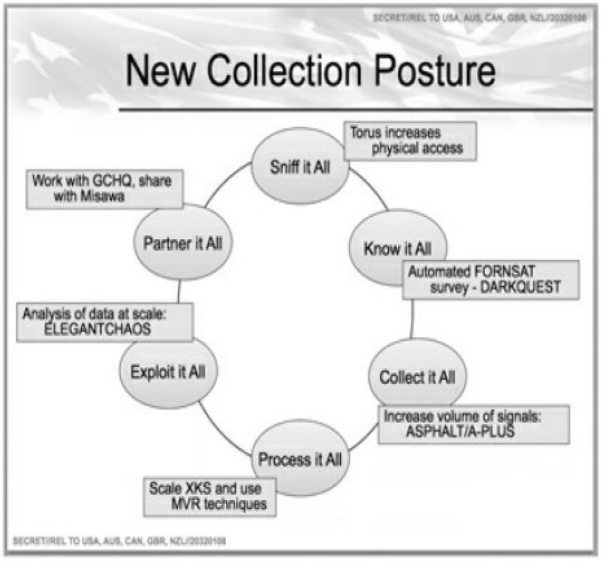
Khẩu hiệu cá nhân của Alexander, "Hãy thu thập tất cả", tuyệt vời truyền đạt mục đích trọng tâm của NSA. Ông ta lần đầu tiên đã đặt ra triết lý này vào thực tế vào năm 2005 khi việc thu thập tình báo dấu hiệu có liên quan tới sự chiếm đóng Iraq. Như tờ *Washington Post* đã nêu trong năm 2013, Alexander đã trở nên không thỏa mãn với trọng tâm có giới hạn của tình báo quân sự Mỹ, nó chỉ nhằm vào những người nổi loạn bị tình nghi và các mối đe dọa khác đối với các lực lượng Mỹ, một

tiếp cận lãnh đạo mới được bổ nhiệm được xem là quá ép buộc. "Ông ta đã muốn mọi điều: từng thông điệp văn bản của Iraq, cuộc gọi điện thoại, và thư điện tử mà có thể bay vào chân không với các máy tính mạnh của cơ quan này". Vì thế chính phủ đã triển khai các phương pháp công nghệ bừa bãi để thu thập tất cả các dữ liệu truyền thông từ toàn bộ dân chúng Iraq.

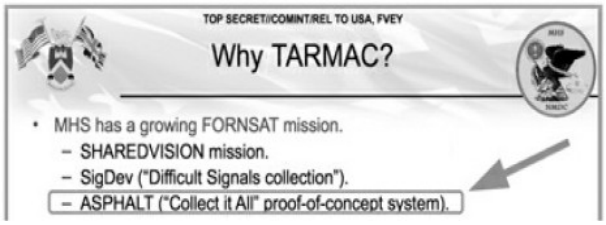
Alexander sau đó đã truyền đạt việc áp dụng hệ thống giám sát khắp mọi nơi này - ban đầu được tạo ra cho dân chúng nước ngoài trong một vùng chiến sự đang hoạt động - tới các công dân Mỹ. "Và, như ông ta đã làm ở Iraq, Alexander đã thúc cật lực vì bất kỳ điều gì ông ta có thể có", tờ *Washington Post* đã nêu: "các công cụ, các tài nguyên, và quyền pháp lý để thu thập và lưu trữ lượng khổng lồ các thông tin thô về các giao tiếp truyền thông của nước ngoài và Mỹ". Như vậy, "trong 8 năm của ông ta ở trên đỉnh của cơ quan giám sát điện tử quốc gia, Alexander, 61 tuổi, đã âm thầm điều khiển qua một cuộc cách mạng trong khả năng của chính phủ để nạo vét thông tin nhân danh an ninh quốc gia".

Uy tín của Alexander như một kẻ cực đoan giám sát được ghi chép lại tốt. Trong việc mô tả "chỉ sự dẫn dắt pháp lý của ông ta để xây dựng bộ máy gián điệp lớn nhất", báo *Chính sách Đối ngoại* đã gọi ông ta là "tên cao bồi của NSA". Thậm chí lãnh đạo NSA và CIA thời tổng thống Bush, tướng Michael Hayden - người bản thân mình trông coi sự triển khai chương trình nghe lén không đảm bảo và bất hợp pháp của Bush và là hiển nhiên đối với chủ nghĩa quân phiệt hung hăng của ông - đã thường có "chứng ợ nóng" về tiếp cận không cầm nén được của Alexander, theo báo *Chính sách Đối ngoại*. Một cựu quan chức tình báo đặc tả quan điểm của Alexander: "Hãy đừng lo về luật. Hãy chỉ ra cách để công việc được hoàn thành". Tờ *Washington Post* cũng đã lưu ý tương tự rằng "thậm chí những người bảo vệ ông ta nói tính hung hăng của Alexander đôi khi làm cho ông ta đi quá giới hạn quyền pháp lý của ông ta".

Dù một số tuyên bố cực đoan hơn từ Alexander - như câu hỏi lỗ mãng của ông ta "Vì sao không thể thu thập tất cả các dấu hiệu, tất cả mọi lúc?", mà ông ta được cho là đã hỏi trong chuyến viếng thăm năm 2008 tới GCHQ của Anh - từng được người phát ngôn của cơ quan này bỏ qua như chỉ là sự châm biếm vui vẻ nằm ngoài ngữ cảnh, thì các tài liệu của riêng cơ quan này trình bày rằng Alexander đã không đùa. Một trình chiếu tuyệt mật cho hội nghị thường niên năm 2011 của liên minh 5 cặp mắt, ví dụ, chỉ ra rằng NSA đã rõ ràng ôm lấy khẩu hiệu của Alexander về mọi sự như là mục tiêu cốt lõi của nó:



Một tài liệu năm 2010 đã trình bày cho hội nghị của 5 cặp mắt từ GCHQ - tham chiếu tới chương trình đang diễn ra để can thiệp các giao tiếp truyền thông vệ tinh, có tên mã là TARMAC - làm rõ rằng cơ quan gián điệp Anh cũng sử dụng câu này để mô tả nhiệm vụ của nó:



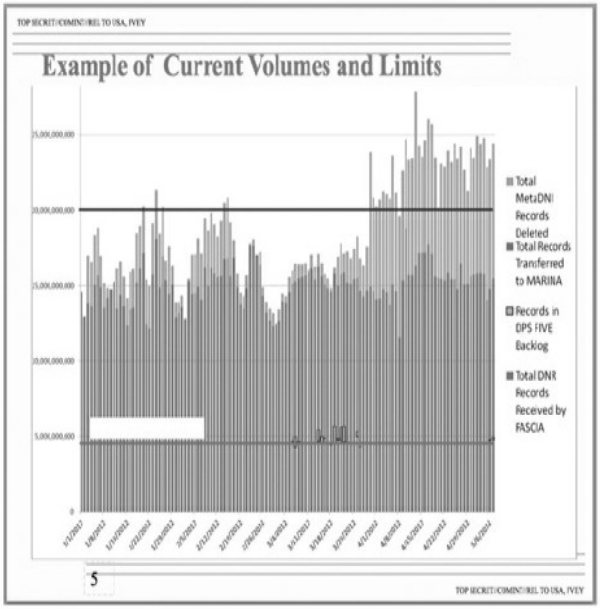
Thậm chí các bản ghi nhớ thường lệ trong nội bộ NSA cũng viện dẫn khẩu hiệu đó để minh chứng cho việc mở rộng các khả năng của cơ quan này. Một bản ghi nhớ năm 2009 từ giám đốc kỹ thuật các Tác chiến Nhiệm vụ của NSA, ví dụ, động chạm tới các cải tiến gần đây đối với site thu thập của cơ quan này ở Misawa, Nhật Bản:

Future Plans (U)

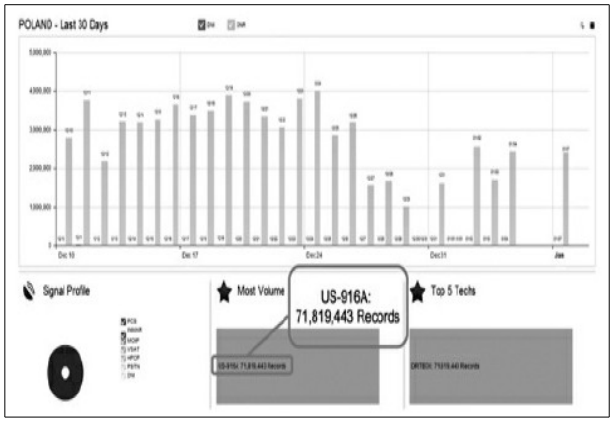
(TS//SI//REL) In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers.

These targets are ideally suited for software demodulation. Additionally, MSOC has developed a capability to automatically scan and demodulate signals as they activate on the satellites. There are a multitude of possibilities, bringing our enterprise one step closer to "collecting it all."

Ngoài một lời châm biếm phù phiếm, "thu thập tất cả" xác định khát vọng của NSA, và nó là mục tiêu mà NSA đang ngày càng gần đạt được tới. Số lượng các cuộc gọi điện thoại, thư điện tử, hội thoại tức thời (chat) trực tuyến, các hoạt động trực tuyến, và các siêu dữ liệu điện thoại được cơ quan này thu thập là làm choáng người. Quả thực, NSA thường xuyên, như một tài liệu đưa ra, "thu thập nội dung nhiều hơn nhiều so với 20 tỷ sự kiện truyền thông (cả Internet và điện thoại) từ khắp thế giới *mỗi ngày*":



Đối với từng quốc gia riêng rẽ, NSA cũng tạo ra một kỷ lục hàng ngày bằng việc định lượng số lượng các cuộc gọi và thư điện tử thu thập được. Đồ thị bên dưới, đối với Balan, chỉ ra nhiều hơn 3 triệu cuộc gọi điện thoại trong vài ngày, cho tổng số 30 ngày là 71 triệu cuộc:



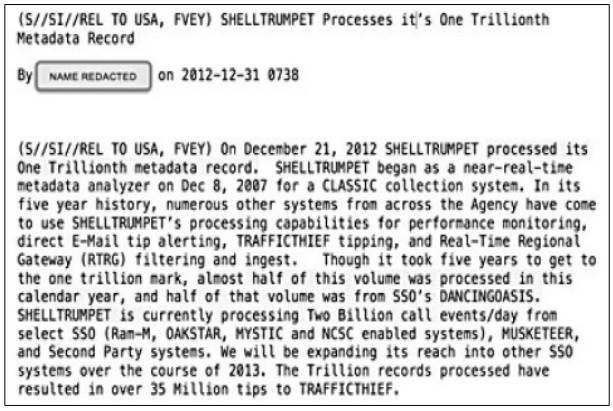
Tổng cộng các cuộc trong nội địa được NSA thu thập gây choáng váng ngang bằng. Thậm chí trước cả các phát hiện của Snowden, tờ *Washington Post* đã nêu trong năm 2010 rằng "mỗi ngày, các hệ thống thu thập ở NSA can thiệp và lưu trữ 1.7 tỷ thư điện tử, các cuộc gọi điện thoại, và các dạng giao tiếp truyền thông khác" từ những người Mỹ. William Binney, một nhà toán học từng làm việc cho NSA 3 thập kỷ và đã từ nhiệm trong làn sóng ngày 11/09 để phản đối sự tập trung ngày một gia tăng vào nội địa của cơ quan này, cũng đã đưa ra vô số các tuyên bố về số lượng các dữ liệu Mỹ được thu thập. Trong một cuộc phỏng vấn năm 2012 với *Dân chủ Bây giờ* (*Democracy Now!*), Binney đã nói rằng "họ đã thu thập khoảng 20 ngàn tỷ giao dịch của các công dân Mỹ với các công dân Mỹ khác".

Sau những tiết lộ của Snowden, *Tạp chí Phố Uôn* (*Wall Street Journal*) đã nêu rằng toàn bộ hệ thống can thiệp trong NSA "có khả năng đạt được khoảng 75% tất cả giao thông Internet của Mỹ

trong cuộc săn lùng tình báo nước ngoài, bao gồm một dải rộng lớn các giao tiếp truyền thông của những người nước ngoài và những người Mỹ". Nói một cách nặc danh, các quan chức NSA trước kia và hiện nay đã nói cho tạp chí rằng trong một số trường hợp NSA "giữ các nội dung văn bản các thư điện tử được gửi giữa các công dân bên trong nước Mỹ và cũng lọc các cuộc gọi điện thoại nội địa được thực hiện với công nghệ Internet".

GCHQ của Anh thu thập tương tự số lượng lớn như vậy các dữ liệu truyền thông mà nó có thể hoàn toàn lưu trữ được những gì nó có. Như một tài liệu năm 2011 được nước Anh chuẩn bị đã đưa ra:

NSA là quá gắn bó với việc thu thập tất cả những gì mà kho lưu trữ của Snowden rắc ra với các bản ghi nhớ kỷ niệm trong nội bộ báo trước các cột mốc thu thập đặc biệt. Một khoản vào tháng 12/2012 từ một bảng thông điệp nội bộ, ví dụ, tự hào tuyên bố rằng chương trình SHELLTRUMPET đã xử lý bản ghi thứ 1 ngàn tỷ của nó:


(S//SI//REL TO USA, FVEY) SHELLTRUMPET Processes it's One Trillionth Metadata Record

By [NAME REDACTED] on 2012-12-31 0738

(S//SI//REL TO USA, FVEY) On December 21, 2012 SHELLTRUMPET processed its One Trillionth metadata record. SHELLTRUMPET began as a near-real-time metadata analyzer on Dec 8, 2007 for a CLASSIC collection system. In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring, direct E-Mail tip alerting, TRAFFICTHIEF tipping, and Real-Time Regional Gateway (RTRG) filtering and ingest. Though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year, and half of that volume was from SSO's DANCINGOASIS. SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems), MUSKETEER, and Second Party systems. We will be expanding its reach into other SSO systems over the course of 2013. The Trillion records processed have resulted in over 35 Million tips to TRAFFICTHIEF.

* * *

Để thu thập số lượng các giao tiếp truyền thông nhiều khổng lồ như vậy, NSA dựa vào vô số các phương pháp. Chúng bao gồm việc áp trực tiếp vào các đường cáp quang (bao gồm cả các cáp ngầm dưới đáy biển) được sử dụng để truyền các giao tiếp truyền thông quốc tế; tái định tuyến các thông điệp vào trong các kho của NSA khi chúng truyền ngang qua hệ thống của Mỹ, như hầu hết các giao tiếp truyền thông trên thế giới làm; và cộng tác với các cơ quan dịch vụ tình báo ở các nước khác. Với tần suất ngày một gia tăng, cơ quan này cũng dựa vào các công ty Internet và viễn thông, họ nhất thiết truyền thông tin mà họ đã thu thập được về các khách hàng của riêng họ.

Trong khi NSA chính thức là một cơ quan nhà nước, thì nó đang có vô số các đối tác chồng chéo

với các tập đoàn khu vực tư nhân, và nhiều trong số các chức năng cốt lõi của nó đã được đưa ra thuê ngoài làm. Bản thân NSA thuê gần 30.000 người, nhưng cơ quan cũng đã ký hợp đồng với khoảng 60.000 nhân viên của các tập đoàn tư nhân, những người thường cung cấp các dịch vụ cơ bản. Bản thân Snowden thực sự từng được thuê không phải do NSA mà do tập đoàn Dell và nhà thầu quân sự lớn Booz Allen Hamilton. Hơn nữa, anh ta, giống như nhiều nhà thầu tư nhân khác, đã làm việc trong các văn phòng của NSA, trong các chức năng cốt lõi của nó, với sự truy cập tới các bí mật của nó.

Theo Tim Shorrock, người từ lâu ghi chép biên niên sử mối quan hệ với các tập đoàn của NSA thì "70% ngân sách tình báo quốc gia đang được chi cho khu vực tư nhân". Khi Michael Hayden nói rằng "sự tập trung lớn nhất sức mạnh không gian mạng trên thế giới là sự giao cắt của Baltimore Parkway và Maryland Route 32", thì Shorrock đã lưu ý, "ông ta từng tham chiếu không phải tới bản thân NSA mà tới công viên các doanh nghiệp nằm cách khoảng 1 dặm xuống phía đường từ công trình xây dựng đen khổng lồ mà sở chỉ huy của NSA nằm tại Fort Meade, Md. Ở đó, tất cả các nhà thầu chính của NSA, từ Booz tới SAIC tới Northrop Grumman, triển khai công việc giám sát và tình báo của họ cho cơ quan này".

Các mối quan hệ tập đoàn đó mở rộng vượt ra khỏi các nhà thầu tình báo và quốc phòng để bao gồm các tập đoàn Internet và viễn thông quan trọng nhất và lớn nhất thế giới, chính xác các công ty đó điều khiển phần lớn các giao tiếp truyền thông thế giới và có thể tạo thuận lợi cho sự truy cập tới thị trường chứng khoán tư nhân. Sau việc mô tả các nhiệm vụ của cơ quan về "Phòng vệ (Bảo vệ các Hệ thống Viễn thông và Máy tính Mỹ Chống lại sự Khai thác)" và "Tấn công (Can thiệp và Khai thác các Dấu hiệu Nước ngoài)" (Defense (Protect U.S. Telecommunications and Computer Systems Against Exploitation)" and "Offense (Intercept and Exploit Foreign Signals), một tài liệu tuyệt mật của NSA liệt kê một vài dịch vụ được các tập đoàn như vậy cung cấp:

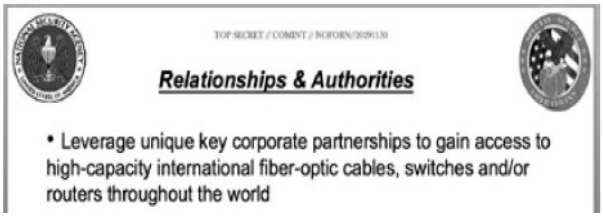
Các mối quan hệ tập đoàn đó cung cấp các hệ thống và sự truy cập mà NSA phụ thuộc vào, được đơn vị Tác chiến Nguồn Đặc biệt - SSO (Special Sources Operations) bí mật cao độ của NSA quản lý, bộ phận trông nom các mối quan hệ tập đoàn.

Snowden đã mô tả SSO như là "viên ngọc trên vương miện" của tổ chức này.

BLARNEY, FAIRVIEW, OAKSTAR, và STORMBREW là vài trong số các chương trình được SSO trông nom bên trong hồ sơ Truy cập Đối tác Tập đoàn - CPA (Corporate Partner Access) của mình.

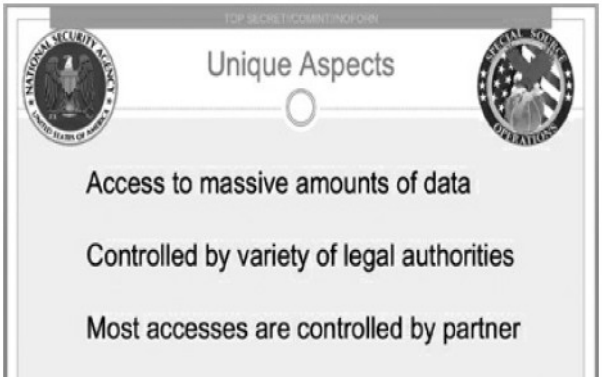
Như một phần của các chương trình đó, NSA khai thác sự truy cập mà các công ty viễn thông nhất định có đối với các hệ thống quốc tế, tham gia vào các hợp đồng với các nhà viễn thông nước ngoài để xây dựng, duy trì và nâng cấp các mạng của họ. Các công ty Mỹ sau đó tái định tuyến các dữ liệu các giao tiếp truyền thông của các quốc gia đích tới các kho của NSA.

Mục đích cốt lõi của BLARNEY được miêu tả trong một bản tóm tắt của NSA:



BLARNEY đã dựa vào một mối quan hệ đặc biệt - mối quan hệ dài lâu với AT&T Inc., theo báo cáo của *Tạp chí Phố Uôn* về chương trình này. Theo các tệp của riêng NSA, trong năm 2010 thì danh sách các quốc gia bị BLARNEY ngắm đích gồm có Brazil, Pháp, Đức, Hy Lạp, Israel, Nhật, Mexico, Hàn Quốc và Venezuela, cũng như Ủy ban châu Âu và Liên hiệp quốc.

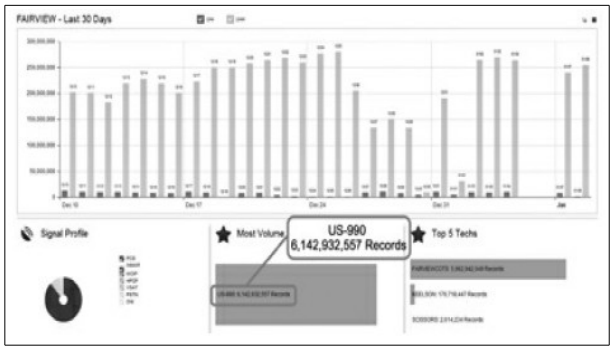
FAIRVIEW, một chương trình khác của SSO, cũng thu thập những gì NSA động tới như là "lượng dữ liệu khổng lồ" từ khắp thế giới. Và nó, cũng vậy, dựa phần lớn vào "đối tác tập đoàn" duy nhất và, đặc biệt, rằng sự truy cập của đối tác tới các hệ thống viễn thông các quốc gia nước ngoài. Tóm tắt nội bộ của NSA về FAIRVIEW là đơn giản và rõ ràng:



Theo các tài liệu của NSA, FAIRVIEW "thường nằm trong 5 chương trình hàng đầu ở NSA như là một nguồn thu thập cho sản xuất được tuần tự hóa" - nghĩa là sự giám sát liên tục - "và là một trong những nhà cung cấp lớn nhất các siêu dữ liệu". Sự nương tựa áp đảo của nó vào một nhà viễn thông được mô tả với tuyên bố rằng "khoảng 75% báo cáo là nguồn duy nhất, phản ánh sự truy cập duy nhất mà chương trình thụ hưởng đối với sự đa dạng lớn các giao tiếp truyền thông đích". Dù nhà viễn thông đó không được nhận diện, thì một mô tả đối tác của FAIRVIEW làm rõ sự say mê của nó để hợp tác:

> FAIRVIEW - Corp partner since 1985 with access to int. cables, routers, switches. The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs. Aggressively involved in shaping traffic to run signals of interest past our monitors.

Cảm ơn sự hợp tác như vậy, chương trình FAIRVIEW thu thập số lượng khổng lồ thông tin về các cuộc gọi điện thoại. Một đồ thị đề cập tới giai đoạn 30 ngày bắt đầu từ 10/12/2012, chỉ ra rằng chỉ một mình chương trình này từng có trách nhiệm về sự thu thập khoảng 200 triệu bản ghi mỗi ngày trong tháng đó, trong tổng số 30 ngày với hơn 6 tỷ bản ghi. Các thanh sáng màu là các thu thập của "DNR" (các cuộc gọi điện thoại), trong khi các thanh tối màu là "DNI" (hoạt động Internet):



Để thu thập hàng tỷ bản ghi điện thoại đó, SSO hợp tác với các đối tác tập đoàn của NSA cũng như với các cơ quan chính phủ nước ngoài - ví dụ, cơ quan dịch vụ tình báo Balan:

(TS//SI//NF) ORANGECRUSH, part of the OAKSTAR program under SSO's corporate portfolio, began forwarding metadata from a third party partner site (Poland) to NSA repositories as of 3 March and content as of 25 March. This program is a collaborative effort between SSO, NCSC, ETC, FAD, an NSA Corporate Partner and a division of the Polish Government. ORANGECRUSH is only known to the Poles as BUFFALOGREEN. This multi-group partnership began in May 2009 and will incorporate the OAKSTAR project of ORANGEBLOSSOM and its DNR capability. The new access will provide SIGINT from commercial links managed by the NSA Corporate Partner and is anticipated to include Afghan National Army, Middle East, limited African continent, and European communications. A notification has been posted to SPRINGRAY and this collection is available to Second Parties via TICKETWINDOW.

Chương trình OAKSTAR tương tự khai thác sự truy cập mà một trong số các đối tác tập đoàn của NSA (tên mã STEELKNIGHT) có đối với các hệ thống viễn thông nước ngoài, bằng việc sử dụng sự truy cập đó để tái định tuyến các dữ liệu vào trong các kho của riêng NSA. Một đối tác khác, tên mã là SILVERZEPHYR, xuất hiện trong một tài liệu đề ngày 11/11/2009 mô tả công việc được thực hiện với công ty để giành được "các giao tiếp truyền thông nội bộ" từ cả Brazil và Colombia.

SILVERZEPHYR FAA DNI Access Initiated at NSAW (TS//SI//NF)

By NAME REDACTED on 2009-11-06 0918

(TS//SI//NF) On Thursday, 11/5/09, the SSO-OAKSTAR SILVERZEPHYR (SZ) access began forwarding FAA DNI records to NSAW via the FAA WealthyCluster2/Tellurian system installed at the partner's site. SSO coordinated with the Data Flow Office and forwarded numerous sample files to a test partition for validation, which was completely successful. SSO will continue to monitor the flow and collection to ensure a ny anomalies are identified and corrected as required. SILVERZEPHYR will continue to provide customers with authorized, transit DNR collection. SSO is working with the partner to gain access to an additional 80Gbs of DNI data on their peering network, bundled in 10 Gbs increments. The OAKSTAR team, along with support from NSAT and GNDA, just completed a 12 day SIGINT survey at site, which identified over 200 new links. During the survey, GNDA worked with the partner to test the output of their ACS system. OAKSTAR is also working with NSAT to examine snapshots taken by the partner in Brazil and Colombia, both of which may contain internal communications for those countries.

Trong khi đó, chương trình STORMBREW, được tiến hành trong "mối quan hệ đối tác gần gũi với FBI", trao cho NSA sự truy cập tới giao thông Internet và điện thoại mà đi vào nước Mỹ ở "các điểm nghẽn" khác nhau trên đất Mỹ. Nó khai thác thực tế rằng đa số lớn giao thông Internet thế giới

ở một vài điểm chảy qua hạ tầng truyền thông của Mỹ - một phần dư sót lại theo sản phẩm của vai trò trung tâm mà nước Mỹ đã đóng trong việc phát triển mạng. Một số trong só đó đã chỉ định các điểm nghẽn được các tên bao trùm nhận diện:

Theo NSA, STORMBREW "hiện bao gồm các mối quan hệ rất nhạy cảm với 2 nhà cung cấp viễn thông Mỹ (các điều khoản bao trùm ARTIFICE và WOLFPOINT)". Ngoài sự truy cập của nó tới các điểm nghẽn nằm ở Mỹ, "chương trình STORMBREW cũng quản lý 2 site truy cập rải cáp tàu ngầm; một ở bờ biển phía tây của nước Mỹ (khái niệm bao trùm, BRECKENRIDGE), và cái kia ở bờ biển phía đông nước Mỹ (khái niệm bao trùm QUAIL-CREEK)".

Khi có nhiều tên bao trùm làm chứng, thì sự nhận diện các đối tác tập đoàn của nó là một trong những bí mật được canh phòng cẩn mật nhất ở NSA. Các tài liệu chứa đựng khóa tới các tên mã đó được cơ quan này bảo vệ cẩn mật và Snowden từng không thể có được nhiều trong số chúng. Tuy nhiên, những tiết lộ của anh ta đã lột bỏ mặt nạ một số công ty hợp tác với NSA. Nổi tiếng nhất, kho lưu trữ của anh ta đã bao gồm các tài liệu PRISM, chúng đã chi tiết hóa các thỏa thuận bí mật giữa NSA và các công ty Internet lớn nhất thế giới - Facebook, Yahoo!, Google - cũng như những nỗ lực của Microsoft để cung cấp cho cơ quan này sự truy cập tới các nền tảng giao tiếp truyền thông của hãng như Outlook.

Không giống như BLARNEY, FAIRVIEW, OAKSTAR, và STORMBREW, chúng kéo theo việc áp vào các cáp quang và các dạng hạ tầng khác (giám sát "ngược lên dòng trên", theo cách nói của NSA), PRISM cho phép NSA thu thập dữ liệu trực tiếp từ các máy chủ của 9 trong số các công ty Internet lớn nhất:

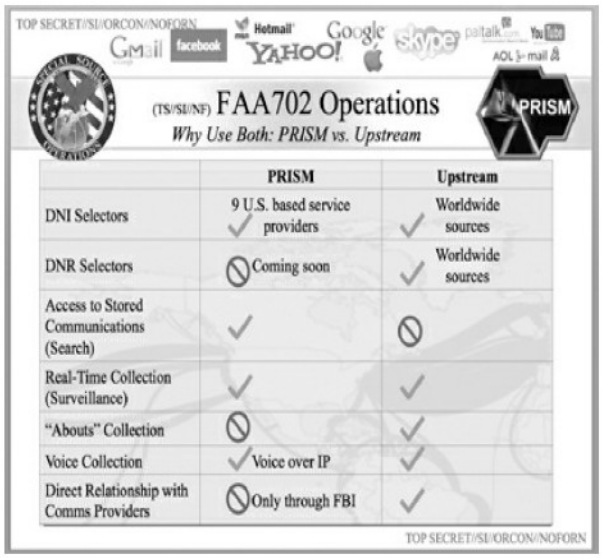
Các công ty được liệt kê trong slide PRISM đã khước từ việc cho phép NSA sự truy cập không hạn chế tới các máy chủ của họ. Facebook và Google, ví dụ, đã nêu rằng họ chỉ trao cho NSA thông tin theo đó cơ quan này có một lệnh cho phép, và đã cố gắng miêu tả PRISM ít hơn là một chi tiết kỹ thuật tầm thường: một hệ thống phân phối được nâng cấp một chút nơi mà NSA nhận được các dữ liệu trong một "hộp khóa" (lockbox) mà các công ty bị ép buộc về pháp lý phải cung cấp.

Nhưng lý lẽ của họ được tin tưởng với vô số điểm. Thứ nhất, chúng ta biết là Yahoo! đã chiến đấu mãnh liệt ở tòa chống lại những nỗ lực của NSA để ép hãng tham gia PRISM - một nỗ lực không chắc có thực nếu chương trình đó đơn giản chỉ là một sự thay đổi vớ vẩn tới hệ thống phân phối. (Những yêu cầu của Yahoo! đã bị tòa án FISA từ chối, và hãng đã bị ra lệnh phải tham gia vào PRISM). Thứ 2, Bart Gellman của tờ *Washington Post*, sau khi nhận được sự chỉ trích nặng nề vì "nói quá" về tác động của PRISM, đã điều tra lại chương trình và đã khẳng định rằng ông bảo lưu tuyên bố trọng tâm của tờ *Washington Post*: "Từ các máy trạm của họ ở bất cứ đâu trên thế giới, các nhân viên chính phủ được phát quang cho sự truy cập của PRISM có thể 'giao nhiệm vụ' cho hệ thống" - đó là, chạy một sự tìm kiếm - "và nhận được các kết quả từ một công ty Internet mà không cần tương tác xa hơn với nhân viên của công ty đó".

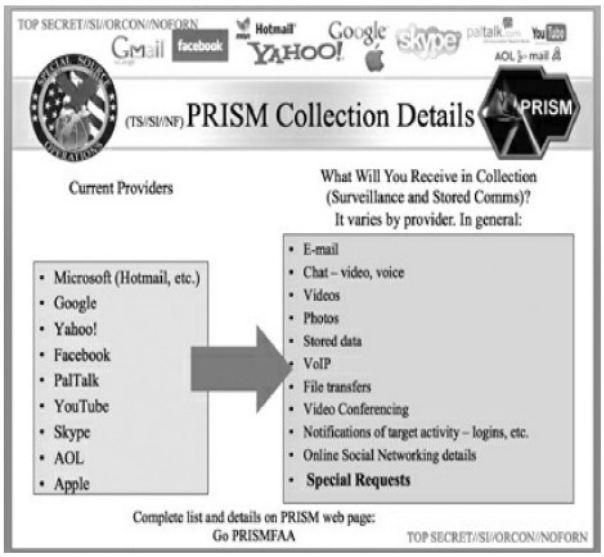
Thứ 3, những lời từ chối của các công ty Internet được diễn đạt theo cách lảng tránh và mang tính pháp lý, thường làm tù mù hơn là làm rõ ràng. Ví dụ, Facebook đã nêu không cung cấp "sự truy cập trực tiếp", trong khi Google đã từ chối đã tạo ra một "cửa hậu" cho NSA. Nhưng như Chris Soghoian, chuyên gia công nghệ của ACLU, đã nói cho báo *Chính sách Đối ngoại*, chúng là các khái niệm nghệ thuật kỹ thuật cao biểu thị ý nghĩa rất đặc thù có được trong thông tin. Các công ty rốt cuộc đã không từ chối rằng họ đã làm việc với NSA để thiết lập một hệ thống qua đó cơ quan này có thể truy cập trực tiếp được tới các dữ liệu khách hàng của họ.

Cuối cùng, bản thân NSA từng tung hô lặp đi lặp lại PRISM về các khả thu thập năng độc nhất vô nhị của nó và đã lưu ý rằng chương trình đó từng là sống còn cho việc gia tăng sự giám sát. Một

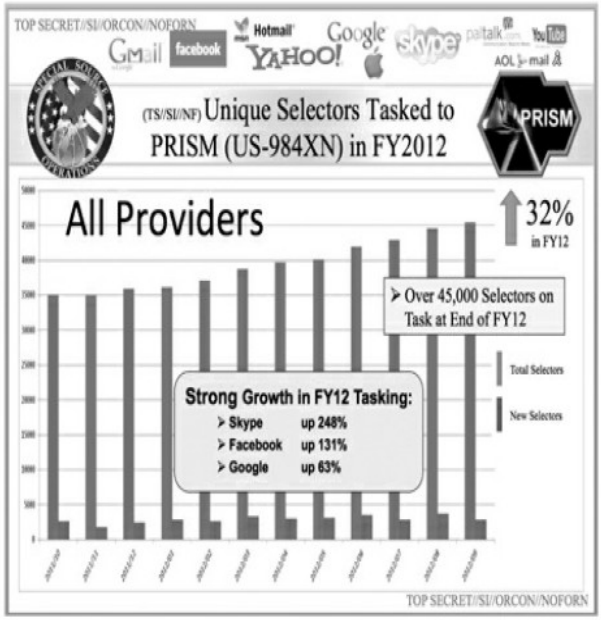
slide của NSA chi tiết hóa sức mạnh giám sát đặc biệt của PRISM:



Một slide khác chi tiết hóa dải rộng lớn các giao tiếp truyền thông mà PRISM cho NSA truy cập:



Và một slide khác của NSA chi tiết hóa cách chương trình PRISM đã gia tăng vững chắc và căn bản sự thu thập của cơ quan này:



Trên bảng điều khiển thông điệp nội bộ của mình, bộ phận Tác chiến Nguồn Đặc biệt thường xuyên tung hô giá trị thu thập ồ ạt mà PRISM đã cung cấp. Một thông điệp, từ ngày 19/11/2012, có đầu đề "PRISM Mở rộng Ảnh hưởng: Đo đếm năm tài chính 2012 (FY12)":

(TS//SI//NF) PRISM (US-984XN) expanded its impact on NSA's reporting mission in FY12 through increased tasking, collection and operational improvements. Here are some highlights of the FY12 PRISM program:

PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA's 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FY11). PRISM was cited in 13.4% of all 1st, 2nd, and 3rd Party NSA reporting (up from 11.9% in FY11), and is also the top cited SIGAD overall

Number of PRISM-based end-product reports issued in FY12: 24,096, up 27% from FY11

Single-source reporting percentage in FY12 and FY11: 74%

Number of product reports derived from PRISM collection and cited as sources in articles in the President's Daily Brief in FY12: 1,477 (18% of all SIGINT reports cited as sources in PDB articles - highest single SIGAD for NSA); In FY11: 1,152 (15% of all SIGINT reports cited as sources in PDB articles - highest single SIGAD for NSA)

Number of Essential Elements of Information contributed to in FY12: 4,186 (32% of all EEIs for all Information Needs); 220 EEIs addressed solely by PRISM

Tasking: The number of tasked selectors rose 32% in FY12 to 45,406 as of Sept 2012

Great success in Skype collection and processing; unique, high value targets acquired

Expanded PRISM taskable e-mail domains from only 40, to 22,000

Những khẳng định chúc mừng như vậy không ủng hộ ý niệm của PRISM chỉ như là một chi tiết kỹ thuật tầm thường, và chúng đưa ra sự lừa dối đối với những từ chối của các tập đoàn Thung lũng Silicon. Quả thực, tờ New York Times, nêu về chương trình PRISM sau các tiết lộ của Snowden, đã mô tả một vũng bùn các thương thảo bí mật giữa NSA và Thung lũng Silicon về việc cung cấp cho cơ quan này sự truy cập không bị cùm xiềng tới các hệ thống của các công ty đó. "Khi các quan chức chính phủ tới Thung lũng Silicon để yêu cầu các cách thức dễ dàng hơn cho các công ty Internet lớn nhất thế giới chuyển qua các dữ liệu người sử dụng như một phần của chương trình giám sát bí mật, các công ty đã xù lông", tờ Times đã nêu. "Cuối cùng, dù vậy, nhiều công ty đã hợp tác ít nhất là một chút". Đặc biệt:

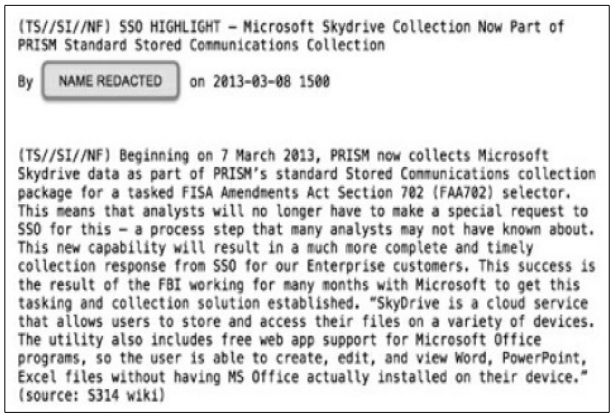
> Twitter đã từ chối làm cho dễ dàng hơn cho chính phủ. Nhưng các công ty khác đã tuân thủ hơn, theo những người đã tóm tắt về các thương thảo đó. Họ đã mở ra các thảo luận với các quan chức an ninh quốc gia về việc phát triển các phương pháp kỹ thuật để chia sẻ được có hiệu quả hơn và an ninh hơn các dữ liệu cá nhân của những người sử dụng là người nước ngoài để đáp lại các yêu cầu phù hợp luật của chính phủ. Và trong một số trường hợp, họ đã thay đổi các hệ thống máy tính của họ để làm được như vậy.

Các thương thảo đó, tờ New York Times nói, "minh họa cách mà chính phủ và các công ty công nghệ làm việc cùng nhau một cách phức tạp, và độ sâu của các giao dịch đằng sau hậu trường của họ". Bài báo cũng tranh luận về các tuyên bố của các công ty rằng họ cung cấp cho NSA chỉ với sự truy cập bị ép buộc theo pháp luật, lưu ý rằng: "Trong khi việc trao các dữ liệu để đáp ứng yêu cầu theo luật FISA là một yêu cầu hợp pháp, thì việc làm cho dễ dàng hơn cho chính phủ để có được thông tin là không phải thế, nó giải thích vì sao Twitter có thể từ chối làm như thế".

Tuyên bố của các công ty Internet rằng họ chuyển cho NSA chỉ các thông tin mà họ được yêu cầu phải cung cấp theo pháp luật cũng đặc biệt là có ý nghĩa. Đó là vì NSA chỉ cần có được một lệnh cho phép riêng rẽ khi nó muốn nhằm đặc biệt tới một người Mỹ. Không có sự cho phép đặc biệt như vậy được yêu cầu đối với cơ quan này để có được các dữ liệu giao tiếp truyền thông của bất kỳ ai không phải người Mỹ trên đất của nước ngoài, *thậm chí khi người đó đang giao tiếp với những người Mỹ*. Tương tự, không có sự kiểm tra hoặc hạn chế trong thu thập hàng đống siêu dữ liệu của NSA, nhờ sự can thiệp của Luật Yêu nước của chính phủ - một sự diễn giải quá rộng mà thậm chí các tác giả gốc ban đầu của luật này từng bị sốc khi biết làm thế nào mà nó đã được sử dụng.

Sự cộng tác chặt chẽ giữa NSA và các tập đoàn tư nhân có lẽ được coi là tốt nhất trong các tài liệu có liên quan tới Microsoft, nó tiết lộ những nỗ lực mạnh mẽ của hãng này để trao cho NSA sự truy cập tới vài trong số các dịch vụ trực tuyến được sử dụng nhiều nhất của hãng, bao gồm cả SkyDrive, Skype, và Outlook.com.

SkyDrive cho phép mọi người lưu trữ các tệp của họ trên trực tuyến và truy cập chúng từ các thiết bị khác nhau, có hơn 250 triệu người sử dụng trên toàn thế giới. "Chúng tôi tin tưởng điều quan trọng là bạn có được sự kiểm soát đối với những ai có thể và không thể truy cập tới các dữ liệu cá nhân của bạn trong đám mây", website SkyDrive của Microsoft tuyên bố. Vâng như một tài liệu của NSA chi tiết hóa, Microsoft đã bỏ ra "nhiều tháng" làm việc để cung cấp cho chính phủ sự truy cập dễ dàng hơn tới các dữ liệu đó:

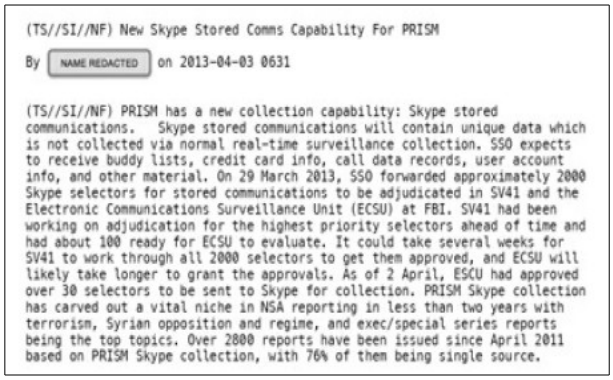


(TS//SI//NF) SSO HIGHLIGHT – Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection

By NAME REDACTED on 2013-03-08 1500

(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)

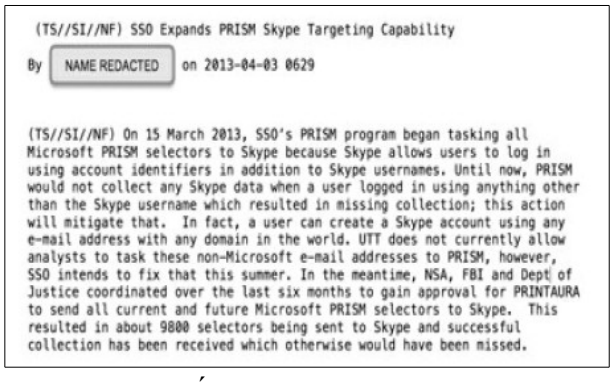
Vào cuối năm 2011, Microsoft đã mua Skype, dịch vụ chat và điện thoại dựa vào Internet với hơn 663 triệu người sử dụng có đăng ký. Vào thời điểm hãng mua nó, Microsoft đã đảm bảo với những người sử dụng rằng "Skype cam kết tôn trọng tính riêng tư và tính bí mật của các dữ liệu cá nhân, giao thông, và nội dung các giao tiếp truyền thông của bạn". Nhưng trong thực tế, các dữ liệu đó, cũng vậy, từng sẵn sàng ngay cho chính phủ. Vào đầu năm 2013, đã có nhiều thông điệp trong hệ thống của NSA chào mừng sự truy cập được cải tiến vững chắc của cơ quan này đối với các giao tiếp truyền thông của những người sử dụng Skype:



(TS//SI//NF) New Skype Stored Comms Capability For PRISM

By NAME REDACTED on 2013-04-03 0631

(TS//SI//NF) PRISM has a new collection capability: Skype stored communications. Skype stored communications will contain unique data which is not collected via normal real-time surveillance collection. SSO expects to receive buddy lists, credit card info, call data records, user account info, and other material. On 29 March 2013, SSO forwarded approximately 2000 Skype selectors for stored communications to be adjudicated in SV41 and the Electronic Communications Surveillance Unit (ECSU) at FBI. SV41 had been working on adjudication for the highest priority selectors ahead of time and had about 100 ready for ECSU to evaluate. It could take several weeks for SV41 to work through all 2000 selectors to get them approved, and ECSU will likely take longer to grant the approvals. As of 2 April, ESCU had approved over 30 selectors to be sent to Skype for collection. PRISM Skype collection has carved out a vital niche in NSA reporting in less than two years with terrorism, Syrian opposition and regime, and exec/special series reports being the top topics. Over 2800 reports have been issued since April 2011 based on PRISM Skype collection, with 76% of them being single source.



(TS//SI//NF) SSO Expands PRISM Skype Targeting Capability

By NAME REDACTED on 2013-04-03 0629

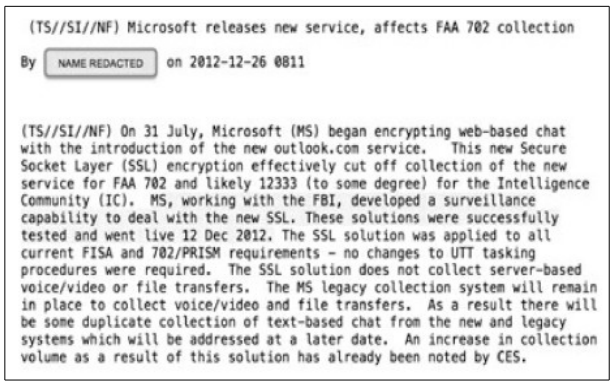
(TS//SI//NF) On 15 March 2013, SSO's PRISM program began tasking all Microsoft PRISM selectors to Skype because Skype allows users to log in using account identifiers in addition to Skype usernames. Until now, PRISM would not collect any Skype data when a user logged in using anything other than the Skype username which resulted in missing collection; this action will mitigate that. In fact, a user can create a Skype account using any e-mail address with any domain in the world. UTT does not currently allow analysts to task these non-Microsoft e-mail addresses to PRISM, however, SSO intends to fix that this summer. In the meantime, NSA, FBI and Dept of Justice coordinated over the last six months to gain approval for PRINTAURA to send all current and future Microsoft PRISM selectors to Skype. This resulted in about 9800 selectors being sent to Skype and successful collection has been received which otherwise would have been missed.

Không chỉ tất cả sự cộng tác này được tiến hành không có sự minh bạch, mà nó đối lập với những tuyên bố công khai mà Skype đã thực hiện. Chuyên gia công nghệ của ACLU Chris Soghoian nói những tiết lộ có thể làm ngạc nhiên nhiều khách hàng của Skype. "Trong quá khứ, Skype đã khẳng định những hứa hẹn đối với những người sử dụng về sự không có khả năng của họ để tiến hành các

vụ nghe lén", ông nói. "Thật khó để sòng phẳng về sự cộng tác bí mật của Microsoft với NSA với những nỗ lực cao của hãng để cạnh tranh về tính riêng tư với Google".

Trong năm 2012, Microsoft đã bắt đầu việc nâng cấp cổng thư điện tử của hãng, Outlook.com, để trộn tất cả các dịch vụ giao tiếp truyền thông của hãng - bao gồm cả Hotmail được sử dụng rộng rãi - thành một chương trình tập trung. Hãng đã chào Outlook mới bằng việc hứa hẹn các mức độ mã hóa cao để bảo vệ tính riêng tư, và NSA đã nhanh chóng có quan ngại lớn rằng sự mã hóa mà Microsoft chào cho các khách hàng Outlook có thể khóa cơ quan này khỏi việc gián điệp trong các giao tiếp truyền thông của họ. Một bản ghi nhớ của SSO từ ngày 22/08/2012, bực bội rằng "việc sử dụng cổng này có nghĩa là việc trộn thư từ nó sẽ bị mã hóa với thiết lập mặc định" và rằng "các phiên chat được tiến hành bên trong cổng đó cũng sẽ được mã hóa khi cả những người giao tiếp cũng sẽ sử dụng một trình chat được mã hóa của Microsoft cho máy trạm".

Nhưng lo lắng đó đã sống được không lâu. Trong vòng ít tháng, 2 thực thể đó đã làm việc cùng nhau và đã tạo ra các phương pháp để NSA phá vỡ được các bảo vệ mã hóa mà Microsoft từng quảng cáo công khai là sống còn cho việc bảo vệ tính riêng tư:



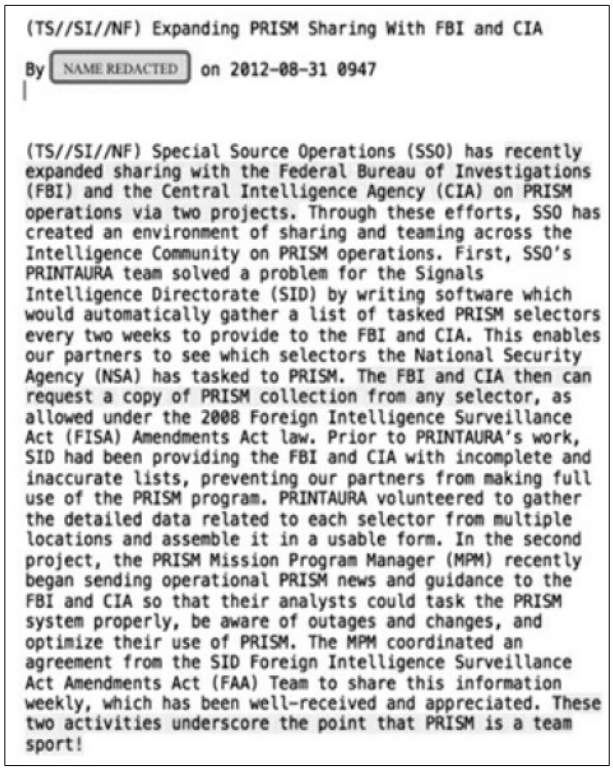
(TS//SI//NF) Microsoft releases new service, affects FAA 702 collection

By NAME REDACTED on 2012-12-26 0811

(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all current FISA and 702/PRISM requirements - no changes to UTT tasking procedures were required. The SSL solution does not collect server-based voice/video or file transfers. The MS legacy collection system will remain in place to collect voice/video and file transfers. As a result there will be some duplicate collection of text-based chat from the new and legacy systems which will be addressed at a later date. An increase in collection volume as a result of this solution has already been noted by CES.

Một tài liệu khác mô tả sự cộng tác xa hơn giữa Microsoft và FBI, khi cơ quan này cũng tìm cách đảm bảo rằng các tính năng mới của Outlook không can thiệp với những thói quen giám sát của hãng: "đội của Đơn vị Công nghệ Can thiệp Dữ liệu - DITU (Data Intercept Technology Unit) của FBI đang làm việc với Microsoft để hiểu một tính năng bổ sung trong Outlook.com mà nó cho phép những người sử dụng tạo các tên hiệu (aliases) thư điện tử, điều có thể ảnh hưởng tới qui trình tác nghiệp của chúng ta... Có các hoạt động được ngăn cách và các hoạt động khác đang diễn ra để giảm nhẹ các vấn đề đó".

Tìm thấy lưu ý này đối với sự giám sát của FBI trong kho lưu trữ của Snowden về các tài liệu nội bộ của NSA từng không phải là một sự việc bị cách li. Toàn bộ cộng đồng tình báo có khả năng truy cập thông tin mà NSA thu thập: nó đều đặn chia sẻ kho dữ liệu khổng lồ của mình với các cơ quan khác, bao gồm cả FBI và CIA. Một mục tiêu cơ bản của cuộc vui lớn của NSA về thu thập dữ liệu từng chính xác là thúc đẩy sự lan truyền thông tin xuyên khắp ban lãnh đạo. Quả thực, hầu như từng tài liệu gắn liền với các chương trình thu thập khác nhau nhắc tới sự tham gia của các đơn vị tình báo khác. Khoản này của năm 2012 từ đơn vị SSO của NSA, về việc chia sẻ các dữ liệu PRISM, hân hoan công bố rằng "PRISM là một đội thể thao!":



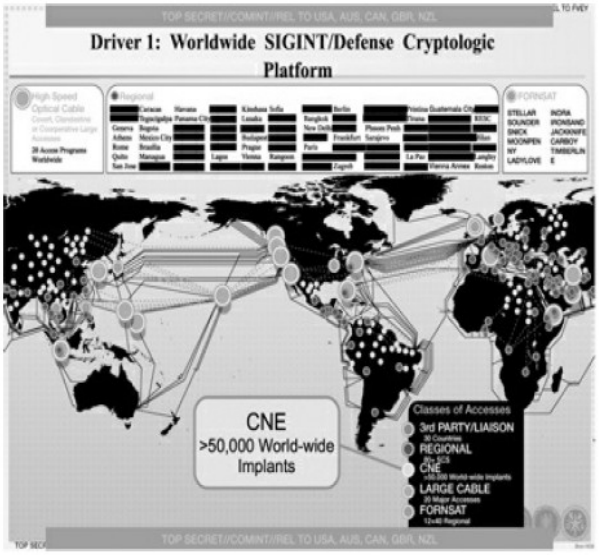
(TS//SI//NF) Expanding PRISM Sharing With FBI and CIA

By NAME REDACTED on 2012-08-31 0947

(TS//SI//NF) Special Source Operations (SSO) has recently expanded sharing with the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) on PRISM operations via two projects. Through these efforts, SSO has created an environment of sharing and teaming across the Intelligence Community on PRISM operations. First, SSO's PRINTAURA team solved a problem for the Signals Intelligence Directorate (SID) by writing software which would automatically gather a list of tasked PRISM selectors every two weeks to provide to the FBI and CIA. This enables our partners to see which selectors the National Security Agency (NSA) has tasked to PRISM. The FBI and CIA then can request a copy of PRISM collection from any selector, as allowed under the 2008 Foreign Intelligence Surveillance Act (FISA) Amendments Act law. Prior to PRINTAURA's work, SID had been providing the FBI and CIA with incomplete and inaccurate lists, preventing our partners from making full use of the PRISM program. PRINTAURA volunteered to gather the detailed data related to each selector from multiple locations and assemble it in a usable form. In the second project, the PRISM Mission Program Manager (MPM) recently began sending operational PRISM news and guidance to the FBI and CIA so that their analysts could task the PRISM system properly, be aware of outages and changes, and optimize their use of PRISM. The MPM coordinated an agreement from the SID Foreign Intelligence Surveillance Act Amendments Act (FAA) Team to share this information weekly, which has been well-received and appreciated. These two activities underscore the point that PRISM is a team sport!

Thu thập "ngược lên dòng trên" (từ các cáp quang) và hướng sự thu thập từ các máy chủ của các công ty Internet (PRISM) tính tới hầu hết các hồ sơ được NSA thu thập. Bổ sung vào sự giám sát quét sạch như vậy, NSA cũng triển khai những gì nó gọi là Khai thác Mạng Máy tính - CNE (Computer Network Exploitation), đặt các phần mềm độc hại vào các máy tính riêng lẻ để giám sát những người sử dụng chúng. Khi cơ quan này thành công trong việc chèn vào các phần mềm độc hại như vậy, có khả năng, theo thuật ngữ của NSA, để "sở hữu" máy tính đó: để xem mọi cú gõ bàn phím được nhập vào và mỗi màn hình được xem. Bộ phận Tác chiến Truy cập Tùy biến - TAO (Tailored Access Operations) có trách nhiệm cho công việc này, trong thực tế, là đơn vị các tin tặc tư nhân của riêng cơ quan này.

Thực tế đột nhập đó là hoàn toàn lan rộng theo quyền của riêng mình: một tài liệu của NSA chỉ ra rằng cơ quan này đã thành công trong việc gây lây nhiễm ít nhất 50.000 máy tính cá nhân với một dạng phần mềm độc hại được gọi là "Chèn Quantum" (Quantum Insertion). Một bản đồ chỉ ra các nơi các tác chiến như vậy từng được thực hiện và số lượng các vụ chèn thành công:



Sử dụng các tài liệu của Snowden, tờ New York Times đã nêu rằng NSA trên thực tế đã cài cắm phần mềm đặc biệt này "vào gần 100.000 máy tính khắp thế giới". Dù phần mềm độc hại đó thường được cài đặt bằng "việc có được sự truy cập tới các mạng máy tính, thì NSA ngày càng tiến hành sử dụng một công nghệ bí mật mà cho phép nó nhập vào và sửa các dữ liệu trong các máy tính thậm chí chúng không được kết nối với Internet".

***

Ngoài công việc của mình với các công ty Internet và viễn thông phục tùng, NSA cũng đã thông đồng với các chính phủ nước ngoài để xây dựng hệ thống giám sát sâu rộng của mình. Nói một cách rộng rãi, NSA có 3 loại khác nhau các mối quan hệ nước ngoài. Trước hết là với nhóm 5 cặp mắt: Mỹ gián điệp với các nước đó, nhưng hiếm khi gián điệp họ, trừ phi được yêu cầu từ các quan chức của riêng các nước đó. Vòng 2 liên quan tới các nước mà NSA làm việc với vì các dự án giám sát đặc biệt trong khi cũng gián điệp họ tích cực. Nhóm thứ 3 bao gồm các nước trong đó Mỹ thường xuyên gián điệp nhưng với những ai mà Mỹ hầu như không bao giờ hợp tác.

Trong nhóm 5 cặp mắt, đồng minh gần nhất của NSA là GCHQ của Anh. Như tờ *Guardian* đã nêu, dựa vào các tài liệu do Snowden cung cấp, "Chính phủ Mỹ đã chi ít nhất 100 triệu £ cho cơ quan gián điệp GCHQ của Anh trong vòng 3 năm qua để đảm bảo anh ninh truy cập tới và gây ảnh hưởng đối với các chương trình thu thập tình báo của Anh". Những khoản thanh toán đó từng là một sự khích lệ cho GCHQ để hỗ trợ cho chương trình hành động giám sát của NSA. "GCHQ phải kéo căng sức của mình và được coi là đã kéo căng sức của mình", một tóm tắt chiến lược bí mật của GCHQ đã nêu.

Các thành viên của 5 cặp mắt chia sẻ hầu hết các hoạt động giám sát của họ và gặp nhau hàng năm ở một hội nghị Phát triển Dấu hiệu (Signals Development), nơi mà họ khoe khoang về sự mở rộng và những thành công năm trước của họ. Cựu Phó giám đốc NSA John Inglis đã nói về liên minh 5 cặp mắt rằng họ "trải nghiệm tình báo trong nhiều điều quan tâm theo một cách thức tổng hợp - cơ bản chắc chắn rằng chúng ta tận dụng được các khả năng của nhau vì lợi ích của các bên".

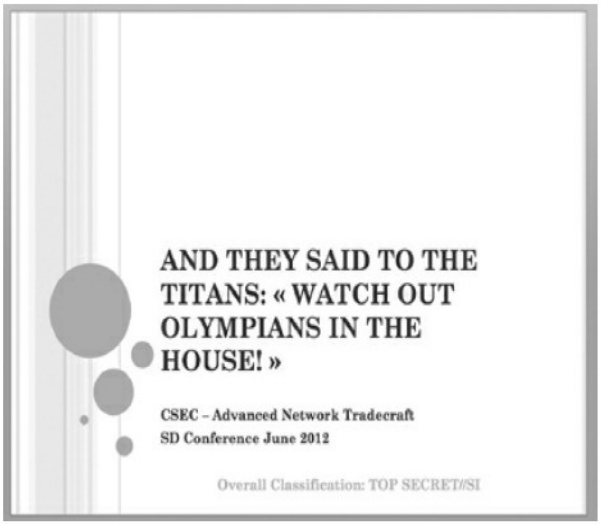
Nhiều chương trình giám sát hăng hái nhất được các đối tác của 5 cặp mắt triển khai, một số lượng đáng kể chúng có liên quan tới GCHQ. Lưu ý đặc biệt là các nỗ lực chung của cơ quan nước Anh với NSA để phá các kỹ thuật mã hóa chung mà sẽ được sử dụng để bảo vệ các giao dịch cá nhân trên Internet, như dịch vụ ngân hàng trực tuyến và truy xuất các hồ sơ y tế. Thành công của 2 cơ quan này trong việc thiết lập truy cập các cửa hậu tới các hệ thống mã hóa đó không chỉ đã cho phép họ bóc được các mối quan hệ giao tiếp riêng tư của mọi người, mà đã còn làm suy yếu các hệ thống đối với từng người, làm cho chúng có khả năng bị tổn thương hơn đối với các tin tặc độc hại và đối với các cơ quan tình báo nước ngoài khác.

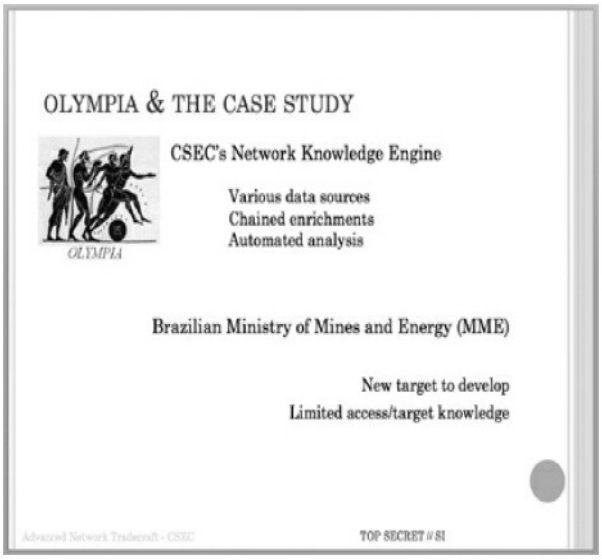
GCHQ cũng đã tiến hành sự can thiệp ồ ạt các dữ liệu truyền thông từ các cáp quang ngầm dưới biển trên thế giới. Dưới cái tên chương trình Tempora, GCHQ đã phát triển "khả năng để áp vào và lưu trữ lượng khổng lồ các dữ liệu được lấy từ các cáp quang tới 30 ngày sao cho nó có thể sàng lọc và phân tích", tờ *Guardian* đã nêu, và "GCHQ và NSA vì vậy có khả năng truy cập và xử lý lượng khổng lồ các giao tiếp truyền thông trong toàn bộ những người vô tội". Các dữ liệu bị can thiệp bao gồm tất cả các dạng hoạt động trực tuyến, bao gồm "các bản ghi các cuộc gọi điện thoại, nội dung các thông điệp thư điện tử, các nội dung trên Facebook, và lịch sử của bất kỳ sự truy cập nào của người sử dụng Internet tới các website".

Các hoạt động giám sát của GCHQ là từng bit một cách toàn diện - và không có trách nhiệm - hệt như của NSA. Như tờ *Guardian* đã nêu:

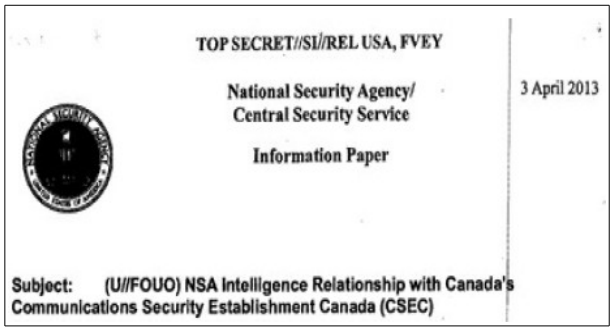
> Phạm vi khổng lồ tham vọng của cơ quan này được phản ánh trong các đầu đề 2 thành phần cơ bản của nó: Làm chủ Internet và Khai thác các hãng Viễn thông Toàn cầu, nhằm vào việc xúc càng nhiều giao thông trực tuyến và điện thoại càng tốt. Tất cả điều này đang được triển khai mà không có bất kỳ dạng thừa nhận công khai hay tranh luận nào.

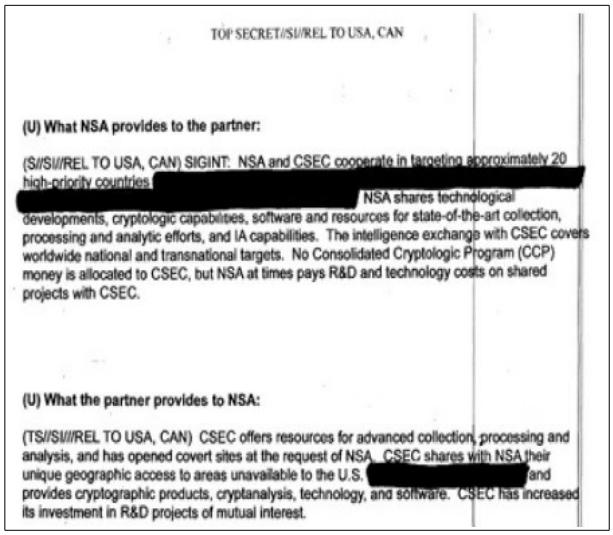
Canada cũng là một đối tác rất tích cực với NSA và là lực lượng giám sát đầy năng lực theo quyền hạn của riêng nó. Tại hội nghị SigDev 2012, Cơ sở Dịch vụ Truyền thông Canada - CSEC (Communications Services Establishment Canada) đã khoe về việc nhằm vào Bộ Mỏ & Năng lượng Brazil, cơ quan của Brazil điều chỉnh nền công nghiệp có lợi ích nhất cho các công ty Canada:





Có bằng chứng hợp tác rộng khắp của CSEC/NSA, bao gồm cả các nỗ lực của Canada để thiết lập các trạm gián điệp để giám sát các giao tiếp truyền thông khắp thế giới theo chỉ thị và vì lợi ích của NSA, và việc gián điệp đối với các đối tác thương mại mà cơ quan Mỹ này nhằm vào.





TOP SECRET//SI//REL TO USA, CAN

(U) What NSA provides to the partner:

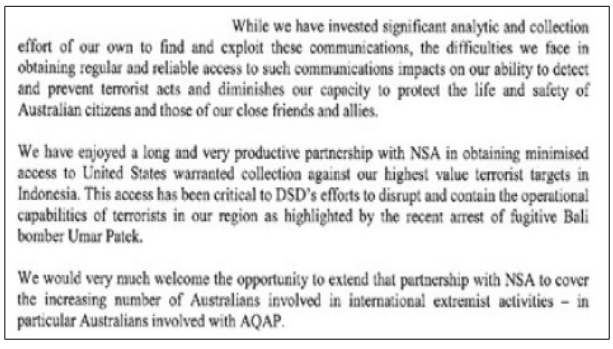
(S//SI//REL TO USA, CAN) SIGINT: NSA and CSEC cooperate in targeting approximately 20 high-priority countries [redacted] NSA shares technological developments, cryptologic capabilities, software and resources for state-of-the-art collection, processing and analytic efforts, and IA capabilities. The intelligence exchange with CSEC covers worldwide national and transnational targets. No Consolidated Cryptologic Program (CCP) money is allocated to CSEC, but NSA at times pays R&D and technology costs on shared projects with CSEC.

(U) What the partner provides to NSA:

(TS//SI//REL TO USA, CAN) CSEC offers resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the U.S. [redacted] and provides cryptographic products, cryptanalysis, technology, and software. CSEC has increased its investment in R&D projects of mutual interest.

Mối quan hệ của 5 cặp mắt gần gũi tới mức mà các chính phủ thành viên đặt các mong muốn của NSA lên trên cả tính riêng tư các công dân của riêng họ. Tờ *Guardian* đã nêu về một bản ghi nhớ năm 2007, ví dụ, mô tả một thỏa thuận "mà đã cho phép cơ quan này 'lột mặt nạ' và giữ lại các dữ liệu cá nhân về những người Anh, điều trước đó từng bị ngăn cấm". Hơn nữa, các qui tắc đã được thay đổi trong năm 2007 "để cho phép NSA phân tích và giữ lại bất kỳ số fax và điện thoại di động nào của các công dân Anh, các thư điện tử và các địa chỉ IP mà mạng lưới của nó quét được".

Đi thêm một bước xa hơn, vào năm 2011 chính phủ Úc rõ ràng đã bênh vực để NSA "mở rộng" quan hệ đối tác của họ và bắt các công dân Úc phải chịu sự giám sát lớn hơn. Trong một bức thư đề ngày 21/02, phó giám đốc điều hành Ban Giám đốc Dấu hiệu Phòng vệ Tình báo (Intelligence Defence Signals Directorate) Úc đã viết cho Ban Giám đốc Tình báo Dấu hiệu của NSA, nói rằng Úc "bây giờ đang đối mặt với một mối đe dọa độc ác và được xác định từ những kẻ cực đoan 'phát triển trong nước' hoạt động tích cực cả trong nước Úc và ở nước ngoài". Ông đã yêu cầu sự giám sát gia tăng đối với các giao tiếp truyền thông của các công dân Úc được cho là bị chính phủ của họ nghi ngờ.



While we have invested significant analytic and collection effort of our own to find and exploit these communications, the difficulties we face in obtaining regular and reliable access to such communications impacts on our ability to detect and prevent terrorist acts and diminishes our capacity to protect the life and safety of Australian citizens and those of our close friends and allies.

We have enjoyed a long and very productive partnership with NSA in obtaining minimised access to United States warranted collection against our highest value terrorist targets in Indonesia. This access has been critical to DSD's efforts to disrupt and contain the operational capabilities of terrorists in our region as highlighted by the recent arrest of fugitive Bali bomber Umar Patek.

We would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities – in particular Australians involved with AQAP.

Ngoài các đối tác của 5 cặp mắt, mức độ hợp tác tiếp theo của NSA là với các đồng minh Lớp B (Tier B): các nước mà có vài hợp tác có giới hạn với cơ quan này và bản thân họ cũng bị ngắm đích

đối với sự giám sát hung hãng, không theo yêu cầu. NSA rõ ràng đã vẽ ra 2 mức đồng minh đó:

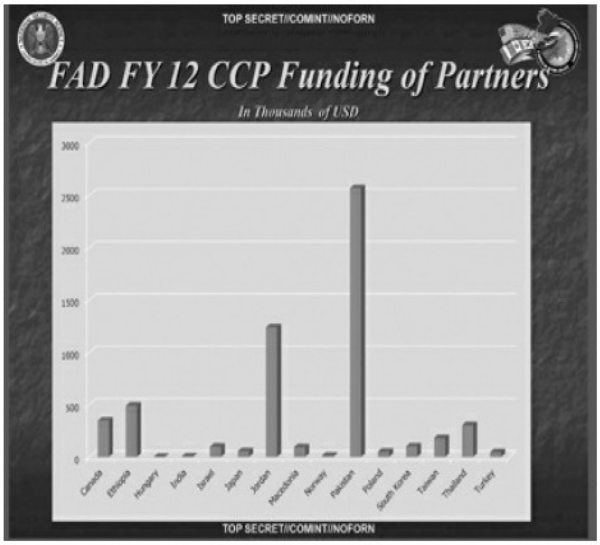
CONFIDENTIAL//NOFORN//20291123

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary
	Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

Sử dụng các phân loại khác nhau (tham chiếu tới Lớp B như là các Bên thứ 3), một tài liệu gần đây của NSA - "Rà soát lại Đối tác Nước ngoài" từ năm tài chính 2013 - chỉ ra một danh sách mở rộng các đối tác của NSA, bao gồm các tổ chức quốc tế như NATO:

Như đối với GCHQ, NSA thường duy trì các mối quan hệ đối tác đó bằng việc trả tiền cho các đối tác của mình để phát triển các công nghệ nhất định và tham gia vào sự giám sát, và có thể vì thế ra lệnh cách mà việc gián điệp được triển khai. "Rà soát lại Đối tác Nước ngoài" năm tài chính 2012 tiết lộ vô số các quốc gia mà đã nhận được các khoản thanh toán như vậy, bao gồm cả Canada,

Israel, Nhật, Jordan, Pakistan, Đài Loan và Thái Lan:

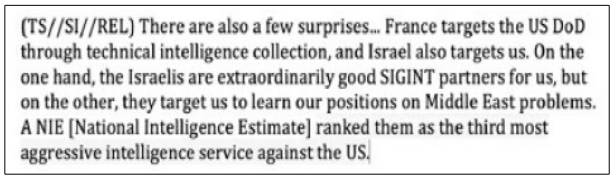


Đặc biệt, NSA có một mối quan hệ đối tác giám sát với Israel mà thường kéo theo sự cộng tác chặt chẽ như mối quan hệ đối tác của 5 cặp mắt, thậm chí đôi lúc còn gần gũi hơn. Một Biên bản Ghi nhớ giữa NSA và cơ quan dịch vụ tình báo Israel chi tiết hóa cách mà nước Mỹ tiến hành bước không bình thường này về việc thường xuyên chia sẻ với Israel thông tin tình báo thô, bao gồm cả các giao tiếp truyền thông của các công dân Mỹ. Trong số các dữ liệu được trao cho Israel là "các bản sao, các yếu điểm, các bản fax, telex, tiếng nói, và siêu dữ liệu và nội dung Tình báo Mạng Số (Digital Network Intelligence) không được định giá và không được giảm thiểu".

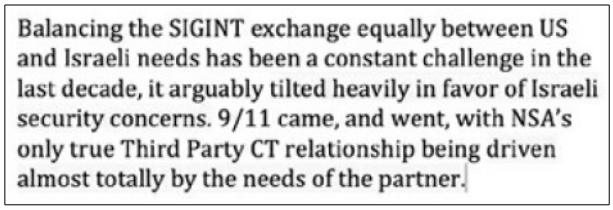
Những gì làm cho việc chia sẻ này đặc biệt khác thường là việc tư liệu đó được gửi cho Israel mà không phải trải qua qui trình "tối thiểu hóa" được yêu cầu theo luật. Các thủ tục tối thiểu hóa được đề xuất để đảm bảo rằng khi sự giám sát ồ ạt của NSA quét qua một số dữ liệu giao tiếp truyền thông thậm chí các chỉ dẫn rất rộng rãi của cơ quan này không cho phép nó được thu thập, như các thông tin sẽ được phá hủy càng sớm càng tốt và không được phổ biến xa hơn. Theo luật, các yêu cầu tối thiểu hóa có nhiều lỗ hổng, bao gồm cả các miễn trừ về "thông tin tình báo nước ngoài quan trọng" hoặc bất kỳ "bằng chứng một sự phạm tội nào". Nhưng khi nó là về việc phổ biến dữ liệu cho tình báo Israel, thì NSA hình như đã phân phối với sự hợp pháp cùng như vậy.

Bản ghi nhớ thẳng thắn nêu: "NSA thường xuyên gửi cho ISNU [Đơn vị Quốc gia SIGINT của Israel] bộ sưu tập thô được tối thiểu hóa và không tối thiểu hóa".

Nhấn mạnh cách mà một nước có thể vừa cộng tác trong giám sát và vừa là một mục tiêu cùng một lúc, một tài liệu của NSA thuật lại lịch sử sự hợp tác của Israel đã lưu ý "các vấn đề tin cậy có liên quan xung quanh các hoạt động ISR trước đó", và đã nhận diện Israel như một trong những cơ quan dịch vụ giám sát hăng hái nhất hành động chống lại nước Mỹ:


(TS//SI//REL) There are also a few surprises... France targets the US DoD through technical intelligence collection, and Israel also targets us. On the one hand, the Israelis are extraordinarily good SIGINT partners for us, but on the other, they target us to learn our positions on Middle East problems. A NIE [National Intelligence Estimate] ranked them as the third most aggressive intelligence service against the US.

Báo cáo y hệt đã quan sát thấy rằng, bất chấp mối quan hệ đối tác gần gũi giữa các cơ quan tình báo Mỹ và Israel, thông tin mở rộng được Mỹ cung cấp cho Israel đã tạo ra ít sự hoàn trả. Tình báo Israel chỉ quan tâm tới việc thu thập các dữ liệu mà giúp được họ. Như NSA đã kêu ca, mối quan hệ đối tác đó từng được gài số "hầu như hoàn toàn" cho các nhu cầu của Israel.


Balancing the SIGINT exchange equally between US and Israeli needs has been a constant challenge in the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party CT relationship being driven almost totally by the needs of the partner.

Một mức khác thấp hơn, theo các đối tác của 5 cặp mắt và các nước lớp thứ 2 như Israel, lớp thứ 3 bao gồm các nước mà thường là các đích ngắm mà không bao giờ là các đối tác của các chương trình gián điệp của Mỹ. Có thể đoán trước chúng bao gồm các chính phủ được xem như là địch thủ, như Trung Quốc, Nga, Iran, Venezuela và Syria. Nhưng lớp thứ 3 cũng bao gồm các nước trải từ thường là thân thiện tới trung lập, như Brazil, Mexico, Argentina, Indonesia, Kenya và Nam Phi.

***

Khi những tiết lộ của NSA lần đầu xuất hiện, chính phủ Mỹ đã cố gắng bảo vệ các hàng động của mình bằng việc nói rằng, không giống các quốc gia nước ngoài, các công dân Mỹ được bảo vệ đối với sự giám sát không có lệnh cho phép của NSA. Vào ngày 18/06/2013, Tổng thống Obama đã nói cho Charlie Rose: "Những gì tôi có thể nói không thể lập lờ nước đôi là nếu bạn là một người Mỹ, thì NSA không thể nghe các cuộc gọi điện thoại của bạn... theo luật và theo qui định, và trừ phi họ ... đi tới một tòa án, và có được một lệnh cho phép, và tìm được lý do có thể, cách y hệt luôn là thế". Chủ tịch Ủy ban Tình báo Hạ viện của GOP, Mike Rogers, đã nói tương tự với CNN rằng NSA "đang không nghe các cuộc gọi điện thoại của những người Mỹ. Nếu nó làm thế, thì điều đó là bất hợp pháp. Nó đang vi phạm luật đấy".

Điều này từng là một dòng bảo vệ khá kỳ lạ: trong thực tế, nó đã nói cho phần còn lại của thế giới rằng NSA đang tấn công vào tính riêng tư của những ai không phải là người Mỹ. Bảo vệ tính riêng tư, hình như, chỉ là cho các công dân Mỹ. Thông điệp này đã nhắc tới sự xúc phạm quốc tế như vậy mà thậm chí CEO Mark Zuckerberg của Facebook, đã không biết chính xác về sự bảo vệ mạnh mẽ tính riêng tư của anh ta, đã than phiền rằng chính phủ Mỹ "đã vi phạm nó" trong trả lời của mình về vụ lùm xùm của NSA bằng việc gây nguy hiểm cho các lợi ích của các công ty Internet quốc tế: "Chính phủ đã nói không lo lắng, chúng tôi đang không gián điệp bất kỳ người Mỹ nào. Tuyệt vời, điều đó thực sự là hữu dụng cho các công ty đang cố gắng làm việc với mọi người trên khắp thế giới. Cảm ơn vì đi ra ngoài đó và là rõ ràng. Tôi nghĩ điều đó thực sự là tồi tệ".

Ngoài việc là một chiến lược kỳ lạ, tuyên bố đó cũng rõ ràng là sai. Trong thực tế, đối nghịch với những từ chối được lặp đi lặp lại của Tổng thống Obama và các quan chức hàng đầu của ông ta, NSA tiếp tục can thiệp vào các giao tiếp truyền thông của các công dân Mỹ mà không có bất kỳ lệnh cho phép cho "lý do có thể" riêng rẽ nào để chứng minh cho sự giám sát như vậy.

Đó là vì luật FISA năm 2008, như được nêu trước đó, cho phép NSA - không có một lệnh cho phép riêng rẽ - theo dõi nội dung của bất kỳ giao tiếp truyền thông của bất kỳ người Mỹ nào miễn là các giao tiếp truyền thông đó được trao đổi với một quốc gia nước ngoài bị ngắm đích. NSA gắn nhãn cho điều này là thu thập "ngẫu nhiên", như thể đó là vài dạng sự cố nhỏ mà cơ quan này đã và đang gián điệp những người Mỹ. Nhưng ngụ ý đó là dối trá. Như Jameel Jaffer, phó giám đốc pháp lý của ACLU, đã giải thích:

> Chính phủ thường nói rằng sự giám sát này đối với các giao tiếp truyền thông của người Mỹ là "chẳng may", điều làm cho nó nghe giống như là sự giám sát của NSA đối với các cuộc gọi điện thoại và thư điện tử của những người Mỹ không phải là cố ý và, thậm chí từ quan điểm của chính phủ, thật là đáng tiếc.
>
> Nhưng khi các quan chức chính quyền Bush đã yêu cầu Quốc hội về sức mạnh giám sát mới này, thì họ đã nói hoàn toàn rõ ràng rằng các giao tiếp truyền thông của những người Mỹ từng là các giao tiếp truyền thông quan tâm nhất đối với họ. Ví dụ, hãy xem FISA cho thế kỷ 21, Điều trần trước Ủy ban Thượng viện về Pháp luật, Quốc hội phiên 109 (2006) (tuyên bố của Michael Hayden), rằng các giao tiếp truyền thông nhất định "với một đầu ở nước Mỹ" là các giao tiếp truyền thông "mà là quan trọng nhất đối với chúng ta".
>
> Mục đích cơ bản của luật 2008 từng là để làm cho có khả năng đối với chính phủ để thu thập các giao tiếp truyền thông quốc tế của những người Mỹ - và để thu thập các giao tiếp truyền thông đó mà không có tham chiếu tới việc liệu có bất kỳ bên nào đối với các giao tiếp truyền thông đó từng làm bất kỳ điều gì bất hợp pháp hay không. Và nhiều sự bảo vệ của chính phủ có ngụ ý để làm mờ đi thực tế này, nhưng đó là một điều cốt tử: Chính phủ không cần phải "ngắm đích" những người Mỹ để thu thập lượng khổng lồ các giao tiếp truyền thông của họ.

Giáo sư Trường Luật Yale Jack Balkin cho rằng luật FISA năm 2008 trao một cách có hiệu lực cho tổng thống quyền để quản lý một chương trình "tương tự có hiệu lực đối với chương trình giám sát không có lệnh cho phép" mà từng được George Bush triển khai bí mật. "Các chương trình đó có thể không tránh khỏi bao gồm nhiều cuộc gọi điện thoại có liên quan tới những người Mỹ, những người có thể tuyệt đối không có liên hệ nào với khủng bố hoặc với Al Qaeda".

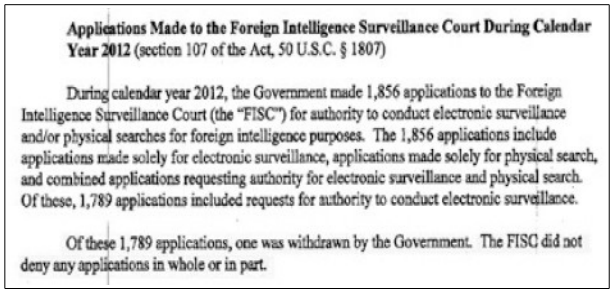
Những đảm bảo làm mất uy tín xa hơn của Obama là dáng bộ khúm núm của tòa án FISA, nó trao cho hầu hết từng yêu cầu giám sát mà NSA đệ trình. Những người bảo vệ NSA thường đưa ra qui trình của tòa án FISA như là bằng chứng rằng cơ quan này nằm dưới sự giám quản có hiệu quả. Tuy nhiên, tòa án đó từng được thành lập không giống như một sự kiểm tra thực sự sức mạnh của chính

phủ, mà như một biện pháp trang trí, cung cấp chỉ vẻ bề ngoài của cải cách để xoa dịu sự tức giận của công chúng đối với các lạm dụng giám sát được tiết lộ trong những năm 1970.

Sự vô dụng của cơ quan này như một sự kiểm tra đúng những lạm dụng giám sát là rõ ràng vì tòa án FISA thiếu gần như mọi thuộc tính của những gì mà xã hội của chúng ta thường hiểu như là những yếu tố tối thiểu của một hệ thống pháp luật. Nó đáp ứng theo sự bí mật hoàn toàn; chỉ một bên - chính phủ - được phép tham dự các cuộc điều trần và tạo ra vụ việc của mình; và các phán quyết của tòa án tự động được chỉ định là "Tuyệt mật". Đáng chú ý, nhiều năm tòa án FISA từng nằm trong Bộ Tư pháp, làm rõ vai trò của nó như một phần của nhánh hành pháp hơn là như một nhánh tư pháp độc lập tiến hành sự giám quản thực sự.

Các kết quả từng chính xác là những gì bạn có thể kỳ vọng: tòa án hầu như không bao giờ từ chối các đề nghị đặc biệt của NSA để tiến hành giám sát nhằm vào những người Mỹ. Ngay từ đầu của nó, FISA đã từng chủ yếu như là cái triện cao su. Trong 24 năm đầu của nó, từ 1978 tới 2002, tòa án đã từ chối tổng cộng 0 (không) đề xuất của chính phủ trong khi phê chuẩn nhiều ngàn đề xuất. Trong thập niên tiếp sau, qua năm 2012, tòa án đã từ chối chỉ 11 đề xuất của chính phủ. Tổng cộng, nó đã phê chuẩn hơn 20.000 đề xuất.

Một trong các điều khoản của luật FISA 2008 yêu cầu nhánh hành pháp thường niên mở ra cho Quốc hội về số lượng các đề xuất nghe lén mà tòa án nhận được và sau đó phê chuẩn, sửa đổi hoặc từ chối. Sự mở ra đó cho năm 2012 đã chỉ ra rằng tòa án đã phê chuẩn từng đơn trong 1.788 đề xuất về giám sát điện tử mà nó đã cân nhắc, trong khi "việc sửa đổi" - đó là, làm hẹp lại phạm vi hiệu lực của lệnh - chỉ trong 40 trường hợp, hoặc ít hơn 3%.



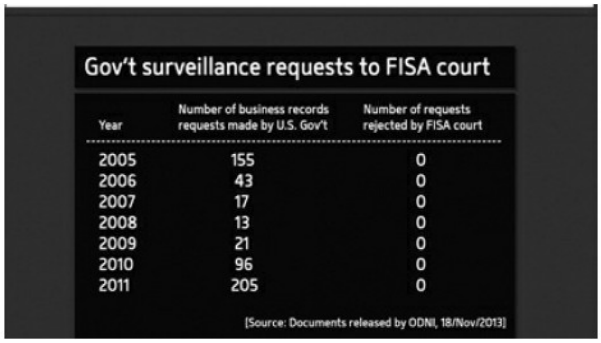
Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2012, the Government made 1,856 applications to the Foreign Intelligence Surveillance Court (the "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,856 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,789 applications included requests for authority to conduct electronic surveillance.

Of these 1,789 applications, one was withdrawn by the Government. The FISC did not deny any applications in whole or in part.

Nhiều điều y hệt từng là đúng vào năm 2011, khi NSA đã nêu 1.676 đề xuất; tòa án FISA, trong khi sửa đổi 30 trong số đó, "đã không từ chối tổng thể hoặc một phần bất kỳ đề xuất nào".

Sự quỵ lụy của tòa án đối với NSA cũng được thể hiện bằng các con số thống kê. Ví dụ, đây là phản ứng của tòa án FISA trong 6 năm vừa qua đối với các yêu cầu khác nhau được NSA thực hiện theo Luật Yêu nước (Patriot Act) để có được các bản ghi của các doanh nghiệp - điện thoại, tài chính hoặc y tế - của những người Mỹ:



Gov't surveillance requests to FISA court

Year	Number of business records requests made by U.S. Gov't	Number of requests rejected by FISA court
2005	155	0
2006	43	0
2007	17	0
2008	13	0
2009	21	0
2010	96	0
2011	205	0

[Source: Documents released by ODNI, 18/Nov/2013]

Vì vậy, thậm chí trong các trường hợp có giới hạn đó khi phê chuẩn từ tòa án FISA là cần thiết để ngắm đích vào các giao tiếp truyền thông của ai đó, thì qui trình đó như là một vở kịch câm nhiều hơn là một sự kiểm tra có ý nghĩa đối với NSA.

Một lớp giám quản khác đối với NSA được các ủy ban tình báo quốc hội đưa ra với vẻ bề ngoài, cũng được tạo ra sau hậu quả của các lùm xùm giám sát những năm 1970, nhưng chúng thậm chí còn uể oải hơn so với tòa án FISA. Trong khi chúng được dự kiến để tiến hành "sự giám quản theo luật định một cách mạnh mẽ" đối với cộng đồng tình báo, thì các ủy ban này trong thực tế hiện được hầu hết các nhà vận động hành lang chuyên tâm của NSA cầm đầu ở Washington: Đảng viên đảng Dân chủ Dianne Feinstein ở Thượng viện và Đảng viên đảng Cộng hòa Mike Rogers ở Hạ viện. Thay vì đưa ra bất kỳ dạng kiểm tra đối đầu nào đối với các hoạt động của NSA, các ủy ban của Feinstein và Rogers tồn tại trước tiên để bảo vệ và biện hộ bất kỳ điều gì mà cơ quan này làm.

Như Ryan Lizza của tờ *New York Times* đã đưa điều này ra trong bài báo tháng 12/2013, thay vì đưa ra sự giám quản, ủy ban Thượng viện thường "ứng xử nhiều hơn với các quan chức tình báo cao cấp như là những thần tượng của các cuộc biểu diễn". Các nhà quan sát các cuộc điều trần tại các ủy ban về các hoạt động của NSA từng bị sốc vì cách mà các thượng nghị sỹ đã tiếp cận khi thẩm vấn các quan chức NSA về việc ai đã xuất hiện trước họ. "Các câu hỏi" thường không có gì ngoài các độc thoại dài dòng của các thượng nghị sỹ về những ký ức của họ về cuộc tấn công ngày 11/09 và là sống còn như thế nào để ngăn chặn các cuộc tấn công trong tương lai. Các thành viên ủy ban đã bỏ qua cơ hội để tra xét các quan chức đó và thực hiện các trách nhiệm giám quản của họ, thay vì việc tuyên truyền theo sự phòng vệ của NSA. Kịch bản đó đã chộp lấy tuyệt vời chức năng đúng đắn của các ủy ban tình báo trong 1 thập kỷ qua.

Quả thực, các chủ tọa của các ủy ban quốc hội đôi khi đã bảo vệ NSA thậm chí còn mạnh mẽ hơn so với bản thân các quan chức của cơ quan đó đã làm. Có lúc, vào tháng 08/2013, 2 thành viên của Quốc hội - Đảng viên đảng Dân chủ Alan Grayson từ Florida và Đảng viên đảng Cộng hòa Morgan Griffith từ Virginia - đã tiếp cận tôi một cách riêng rẽ để phàn nàn rằng Ủy ban Bầu chọn Thường trực Hạ viện về Tình báo (House Permanent Select Committee on Intelligence) từng cô lập họ và các thành viên khác khỏi việc truy cập thông tin cơ bản nhất về NSA. Từng người trong số họ đã trao cho tôi các bức thư mà họ đã viết cho các nhân viên của Chủ tịch Rogers yêu cầu các thông tin về các chương trình của NSA đang được thảo luận trong giới truyền thông. Các yêu cầu đó từng bị

khước từ hết lần này tới lần khác.

Trong làn sóng các câu chuyện Snowden của chúng tôi, một nhóm thượng nghị sỹ từ cả 2 đảng từng có quan tâm từ lâu về những lạm dụng giám sát đã bắt đầu những nỗ lực để phác thảo luật có thể áp đặt những giới hạn thực sự lên sức mạnh của NSA. Nhưng các nhà cải cách đó, được thượng nghị sỹ Đảng dân chủ Ron Wyden từ Oregon dẫn dắt, đã đi vào một con đường cụt ngay lập tức: các phản nỗ lực của những người bảo vệ NSA trong thượng viện để viết luật có thể là cách duy nhất đưa ra sự hiện diện của cải cách, trong khi trong thực tế giữ lại hoặc thậm chí làm gia tăng sức mạnh của NSA. Như Dave Weigel của tờ *Slate* đã nêu hồi tháng 11:

> Các chỉ trích đối với các chương trình giám sát và thu thập dữ liệu tràn lan của NSA không bao giờ lo lắng về sự không hoạt động của quốc hội. Họ đã kỳ vọng Quốc hội đứng lên với thứ gì đó trông giống như sự cải cách nhưng thực tế đã hệ thống hóa và đã xin lỗi các thực tiễn đang được phơi bày và bêu riếu. Đó là những gì luôn xảy ra - mỗi sửa đổi bổ sung hoặc tái ủy quyền cho Luật Yêu nước Mỹ năm 2001 đã xây dựng nhiều cửa hậu hơn là các bức tường.
>
> "Chúng ta sẽ đứng lên chống lại một 'doanh nghiệp thông thường như một lữ đoàn' - đã tạo thành các thành viên có ảnh hưởng đối với lãnh đạo tình báo của chính phủ, các đồng minh của họ trong các nhóm nghiên cứu chiến lược [thinktanks] và giới hàn lâm, các quan chức chính phủ đã về hưu, và các nhà làm luật có sự đồng cảm", thượng nghị sỹ bang Oregon Ron Wyden đã cảnh báo vào tháng trước. "Trò chơi kết thúc của họ đang đảm bảo rằng bất kỳ cải cách giám sát nào cũng chỉ là lớp vỏ... Các bảo vệ tính riêng tư thực sự không bảo vệ tính riêng tư là không đáng để họ in chúng ra giấy".

Phái "cải cách rởm" từng do Dianne Feinstein cầm đầu, thượng nghị sỹ có trách nhiệm với việc thực thi sự giám quản đầu tiên đối với NSA. Feinstein từ lâu đã là một người trung thành chuyên tâm của giới công nghiệp an ninh quốc gia Mỹ, từ sự hỗ trợ mãnh liệt của bà cho cuộc chiến ở Iraq cho tới việc ủng hộ kiên định của bà đối với các chương trình của NSA kỷ nguyên Bush. (Chồng bà, trong khi đó, có những đóng góp chính trong nhiều hợp đồng quân sự khác nhau). Rõ ràng, Feinstein từng là một sự lựa chọn tự nhiên để đứng đầu một ủy ban mà nói sẽ triển khai sự giám quản đối với cộng đồng tình báo mà có nhiều năm đã thực hiện chức năng chống ngược lại.

Như vậy, đối với tất cả sự khước từ của chính phủ, NSA không có sức ép đáng kể nào lên những người mà nó có thể gián điệp và cách mà nó gián điệp. Thậm chí khi những sức ép đó tồn tại trên danh nghĩa - khi các công dân Mỹ là các mục tiêu của giám sát - thì qui trình đó phần lớn đã trở thành rỗng tuếch. NSA là cơ quan xỏ lá dứt khoát: được trang bị để làm bất kỳ điều gì nó muốn với rất ít sự kiểm soát, sự minh bạch, hoặc trách nhiệm giải trình.

***

Nói rất rộng, NSA thu thập 2 dạng thông tin: nội dung và siêu dữ liệu. "Nội dung" ở đây tham chiếu tới việc nghe thực sự các cuộc gọi điện thoại của mọi người hoặc đọc các thư điện tử và các cuộc chat trực tuyến của họ, cũng như việc xem hoạt động Internet như việc duyệt các lịch sử và các hoạt

động tìm kiếm. Thu thập "siêu dữ liệu", trong khi đó, có liên quan tới việc tích cóp các dữ liệu về các giao tiếp truyền thông. NSA tham chiếu tới điều đó như là "thông tin về nội dung (nhưng không phải là bản thân nội dung đó)".

Siêu dữ liệu về một thông điệp thư điện tử, ví dụ, ghi lại ai đã gửi thư điện tử cho ai, khi nào thư điện tử đó được gửi đi, và vị trí của người gửi nó đi. Khi nói về các cuộc gọi điện thoại, thì thông tin bao gồm các số điện thoại của người gọi và người nhận, họ đã nói với nhau bao lâu, và thường các vị trí của họ và các dạng thiết bị mà họ đã sử dụng để giao tiếp. Trong một tài liệu về các cuộc gọi điện thoại, NSA đã phác thảo siêu dữ liệu mà nó truy cập và lưu trữ:

Chính phủ Mỹ đã khăng khăng rằng nhiều sự giám sát được tiết lộ trong kho lưu trữ của Snowden có liên quan tới sự thu thập "các siêu dữ liệu, chứ không phải nội dung", cố gắng ngụ ý rằng dạng gián điệp này không phải là bừa bãi - hoặc ít nhất không ở mức độ y hệt như việc can thiệp nội dung. Dianne Feinstein đã rõ ràng lý luận trên tờ *Nước Mỹ Ngày nay* (*USA Today*) rằng thu thập siêu dữ liệu của tất cả các bản ghi điện thoại của người Mỹ "không phải là giám sát" hoàn toàn vì nó "không thu thập nội dung của bất kỳ giao tiếp truyền thông nào".

Các lý lẽ không thành thật đó làm mù mờ đi thực tế rằng giám sát siêu dữ liệu có thể ít nhất bừa bãi như là sự can thiệp nội dung, và thậm chí thường hơn thế. Khi chính phủ biết từng người mà bạn gọi và từng người mà gọi cho bạn, cộng với độ dài chính xác của tất cả các hội thoại điện thoại đó; khi mà nó có thể liệt kê từng trong số các trao đổi thư điện tử của bạn và từng vị trí từ đó các thư điện tử của bạn đã được gửi đi, thì nó có thể tạo ra một bức tranh toàn diện khác thường về cuộc sống của bạn, các liên kết của bạn, và các hoạt động của bạn, bao gồm cả một số thông tin riêng tư và thân thiết nhất của bạn.

Trong một bản khai có tuyên thệ của ACLU thách thức tính hợp pháp của chương trình thu thập siêu dữ liệu của NSA, giáo sư về các công việc công và khoa học máy tính Princeton Edward Felten đã giải thích vì sao giám sát siêu dữ liệu có thể là tiết lộ đặc biệt:

> Cân nhắc ví dụ giả thiết sau: Một phụ nữ trẻ gọi cho bác sĩ phụ khoa của chị; sau đó ngay lập tức gọi cho mẹ chị; sau đó một người đàn ông mà, trong ít tháng trước, chị đã nói chuyện lặp đi lặp lại trên điện thoại sau 11 giờ đêm; sau một cuộc gọi cho một trung tâm kế hoạch gia đình mà cũng chào sự phá thai. Có khả năng một dòng câu chuyện nổi lên có thể không hiển nhiên rõ bằng việc kiểm tra hồ sơ của một cuộc gọi điện thoại duy nhất.

Thậm chí đối với một cuộc gọi điện thoại duy nhất, siêu dữ liệu có thể có nhiều thông tin hơn so với nội dung cuộc gọi đó. Việc nghe một người phụ nữ gọi một phòng khám phá thai có thể không hé lộ điều gì so với việc ai đó khẳng định một cuộc hẹn với một sự xác minh nghe có vẻ chung chung ("Phòng khám Bờ Đông" hoặc "Văn phòng Bác sĩ Jones"). Nhưng siêu dữ liệu đó có thể chỉ ra nhiều hơn thế nhiều: nó có thể tiết lộ định danh của những người đã được gọi. Điều y hệt là đúng đối với các cuộc gọi tới một dịch vụ hẹn hò, một trung tâm những người đồng tính nam và nữ, một phòng khám cai nghiện ma túy, một chuyên gia HIV hoặc một đường dây nóng về chuyện tự sát. Siêu dữ liệu có thể còn lột mặt nạ một cuộc hội thoại giữa một nhà hoạt động xã hội về quyền con người và một người cung cấp tin trong một chế độ áp chế, hoặc một nguồn bí mật gọi một nhà báo để tiết lộ những việc làm sai mức độ cao. Và nếu bạn thường xuyên gọi ai đó muộn vào buổi đêm mà người đó không phải vợ/chồng bạn, thì siêu dữ liệu đó cũng sẽ tiết lộ điều đó. Hơn nữa, nó sẽ ghi lại không chỉ tất cả mọi người với ai bạn giao tiếp và thường xuyên như thế nào, mà còn tất cả những người với họ các bạn bè và những người có liên quan của bạn giao tiếp, tạo ra một bức tranh toàn diện về mạng các liên hệ của bạn.

Quả thực, như giáo sư Felten lưu ý, việc nghe lén các cuộc gọi có thể hoàn toàn khó khăn vì những khác biệt ngôn ngữ, các cuộc hội thoại ngoằn ngoèo khúc khuỷu, sử dụng tiếng lóng hoặc các mã có chủ ý, và các thuộc tính khác mà hoặc theo thiết kế hoặc ngẫu nhiên làm mù mờ đi ý nghĩa. "Nội dung các cuộc gọi còn khó hơn nhiều để phân tích theo một cách thức được tự động hóa vì bản chất tự nhiên phi cấu trúc của chúng", ông viện lý. Ngược lại, siêu dữ liệu là toán học: rõ ràng, chính xác, và vì thế dễ dàng phân tích được. Và như Felten đưa ra, thường là "sự ủy quyền về nội dung":

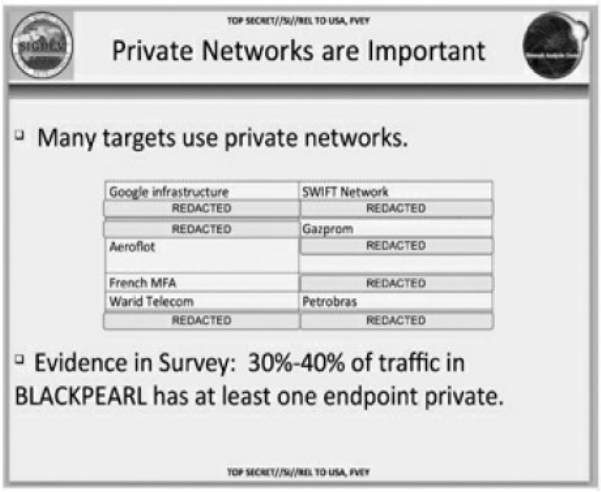
> Siêu dữ liệu của điện thoại có thể ... tiết lộ một lượng lớn khác thường về các thói quen và các mối liên quan của chúng ta. Các mẫu gọi có thể tiết lộ khi nào chúng ta sẽ thức dậy và đi ngủ; tôn giáo của chúng ta, nếu một người thường xuyên không gọi về Sabbath, hoặc có số lượng lớn các cuộc gọi trong ngày lễ Noel; những thói quen trong công việc của chúng ta và thái độ xã hội của chúng ta; số lượng bạn bè mà chúng ta có; và thậm chí các hội đoàn dân sự và chính trị của chúng ta.

Tóm lại, Felten viết, "sự thu thập ồ ạt không chỉ cho phép chính phủ học thông tin về nhiều người hơn, mà nó còn cho phép chính phủ học các sự kiện mới, riêng tư trước đó mà nó có thể đã không học được một cách đơn giản bằng việc thu thập các thông tin về một ít các cá nhân đặc biệt".

Lo lắng về nhiều sự sử dụng mà chính phủ có thể tìm kiếm dạng thông tin nhạy cảm này đặc biệt được minh chứng vì, đối nghịch với những kêu ca lặp đi lặp lại từ Tổng thống Obama và NSA, là rõ ràng rồi rằng một số lượng đáng kể các hoạt động của cơ quan này không có gì phải làm với các nỗ

lực chống khủng bố hoặc thậm chí với an ninh quốc gia. Nhiều điều trong kho lưu trữ của Snowden đã tiết lộ những gì có thể chỉ được gọi là gián điệp kinh tế: việc nghe lén và can thiệp thư điện tử nhằm vào người khổng lồ dầu khí Brazil Petrobras, các hội nghị kinh tế ở Mỹ Latin, các công ty năng lượng ở Venezuela và Mexico, và việc gián điệp của các đồng minh của NSA - bao gồm cả Canada, Nauy và Thụy Điển - vào bộ Mỏ và Năng lượng và các công ty năng lượng Brazil ở vài quốc gia khác.

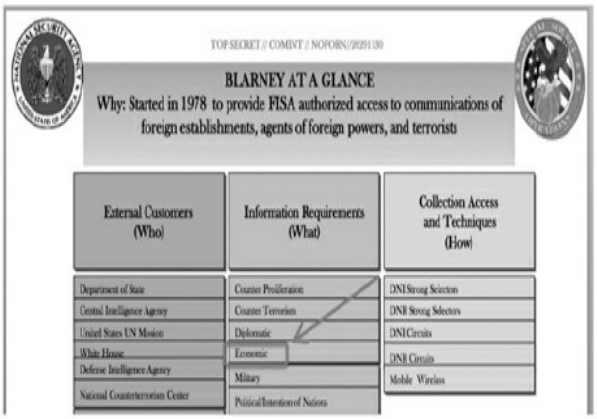
Một tài liệu đáng lưu ý được NSA và GCHQ trình bày chi tiết hóa vô số mục tiêu giám sát từng rõ ràng về kinh tế theo bản chất tự nhiên: Petrobras, hệ thống ngân hàng SWIFT, công ty dầu khí Nga Gazprom, và hãng hàng không Nga Aeroflot.

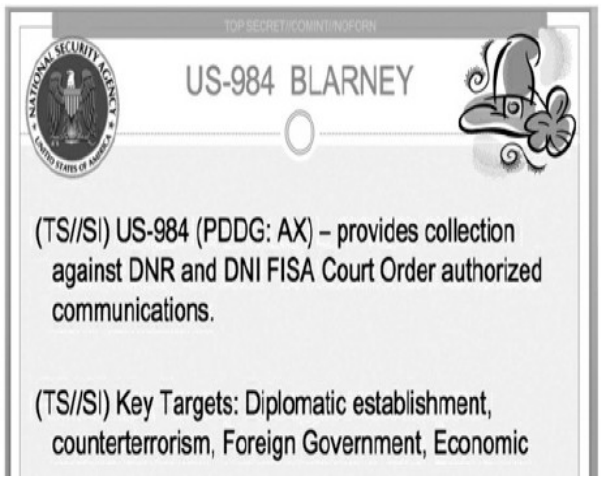


Nhiều năm, Tổng thống Obama và các quan chức hàng đầu của ông đã kịch liệt tố cáo Trung Quốc vì sử dụng các khả năng giám sát của mình cho ưu thế kinh tế trong khi khăng khăng rằng Mỹ và các đồng minh của mình không bao giờ làm bất kỳ điều gì như vậy. Tờ *Washington Post* đã trích lời một người phát ngôn của NSA nói rằng Bộ Quốc phòng Mỹ, mà cơ quan này là một phần của Bộ đó, "'tham gia vào' trong sự khai thác mạng máy tính", nhưng "***không*** tham gia vào gián điệp kinh tế trong bất kỳ lĩnh vực nào, bao gồm cả 'không gian mạng'" [các dấu sao nhấn mạnh theo bản gốc].

Đó là NSA gián điệp chính xác vì động lực kinh tế mà nó đã từ chối được các tài liệu của chính nó chứng minh. Cơ quan này hành động vì lợi ích của những gì mà nó gọi là "các khách hàng" của nó, một danh sách bao gồm không chỉ Nhà Trắng, Bộ Ngoại giao, và CIA, mà còn cả các cơ quan kinh tế hàng đầu, như Đại diện Thương mại Mỹ và Bộ Nông nghiệp, Kho bạc và Thương mại:

Trong mô tả của nó về chương trình BLARNEY, NSA liệt kê các dạng thông tin được cho là cung cấp cho các khách hàng của nó như là "chống khủng bố", "ngoại giao" - và "kinh tế":

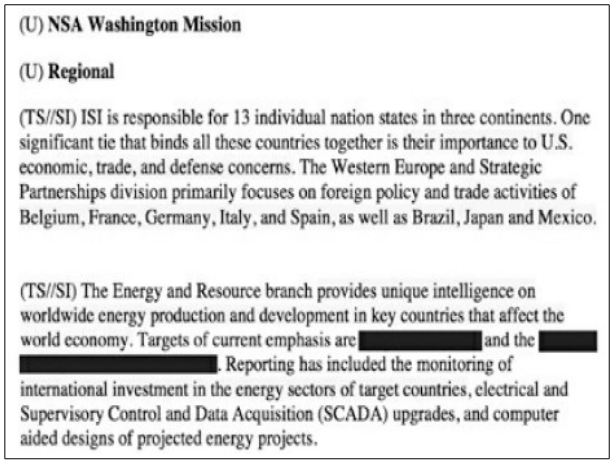




Bằng chứng xa hơn về sự quan tâm kinh tế xuất hiện trong một tài liệu PRISM chỉ ra một "việc lấy mẫu" "các Chủ đề Báo cáo" cho tuần trong khoảng 02-08/02/2013. Một danh sách các dạng thông

tin được thu thập từ các nước khác nhau rõ ràng bao gồm các chủng loại kinh tế và tài chính, trong đó có "năng lượng", "thương mại" và "dầu khí":

Một bản ghi nhớ năm 2006 từ người quản lý các khả năng toàn cầu nhiệm vụ về các Vấn đề An ninh Quốc tế - ISI (International Security Issues) nói về sự gián điệp kinh tế và thương mại của NSA - chống lại các nước khác nhau như Bỉ, Nhật, Brazil và Đức - theo các điều khoản cứng đờ:



(U) **NSA Washington Mission**

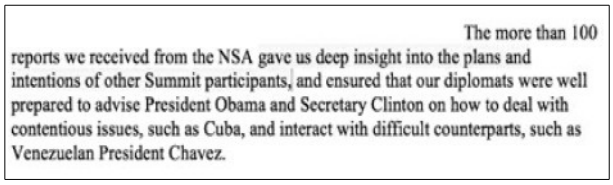
(U) **Regional**

(TS//SI) ISI is responsible for 13 individual nation states in three continents. One significant tie that binds all these countries together is their importance to U.S. economic, trade, and defense concerns. The Western Europe and Strategic Partnerships division primarily focuses on foreign policy and trade activities of Belgium, France, Germany, Italy, and Spain, as well as Brazil, Japan and Mexico.

(TS//SI) The Energy and Resource branch provides unique intelligence on worldwide energy production and development in key countries that affect the world economy. Targets of current emphasis are [redacted] and the [redacted]. Reporting has included the monitoring of international investment in the energy sectors of target countries, electrical and Supervisory Control and Data Acquisition (SCADA) upgrades, and computer aided designs of projected energy projects.

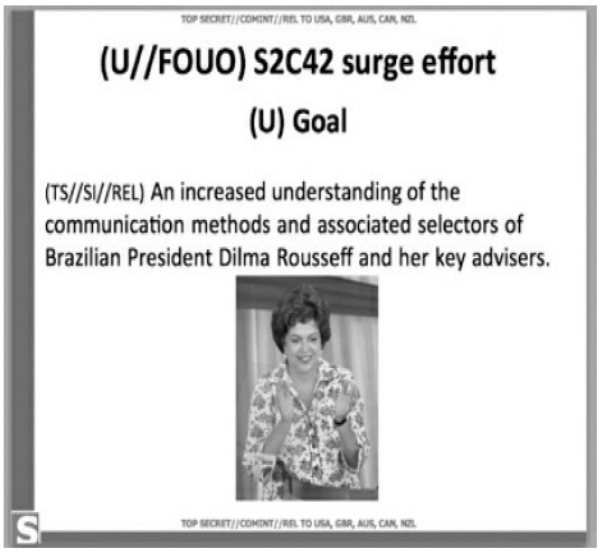
Báo cáo về một nhóm các tài liệu của GCHQ mà Snowden làm rò rỉ, tờ New York Times đã lưu ý rằng các mục tiêu giám sát của nó thường bao gồm các thể chế tài chính và "những người đứng đầu các tổ chức trợ giúp quốc tế, các công ty năng lượng nước ngoài và quan chức của Liên minh châu Âu có liên quan trong các cuộc chiến chống độc quyền với các doanh nghiệp công nghệ Mỹ". Nó đã bổ sụng thêm rằng các cơ quan của Mỹ và Anh "đã theo dõi các giao tiếp truyền thông của các quan chức cao cấp của Liên minh châu Âu, các nhà lãnh đạo nước ngoài, bao gồm cả những người đứng đầu các nhà nước châu Phi và đôi lúc là cả các thành viên gia đình họ, các giám đốc của Liên hiệp quốc và các chương trình giảm nhẹ khác [như UNICEF], và các quan chức giám quản các bộ dầu khí và tài chính".

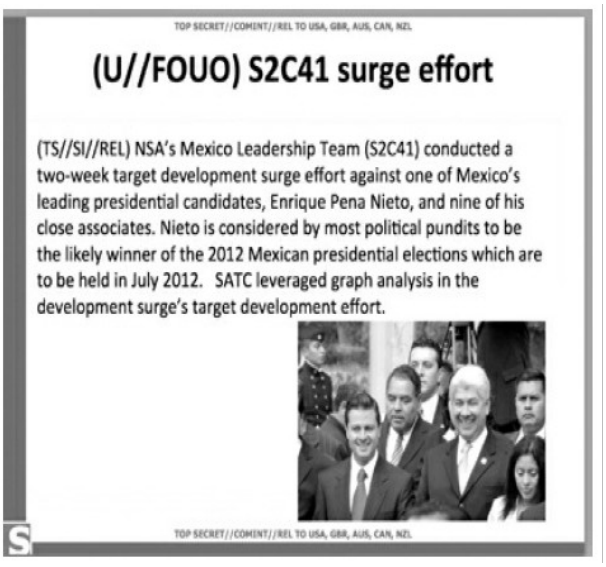
Các lý do cho gián điệp kinh tế là đủ rõ. Khi Mỹ sử dụng NSA để nghe lén trong việc lên kế hoạch các chiến lược của các nước khác trong các cuộc tọa đàm về thương mại và kinh tế, nó có thể giành được ưu thế khổng lồ cho nền công nghiệp Mỹ. Trong năm 2009, ví dụ, Trợ lý Bộ trưởng Ngoại giao Thomas Shannon đã viết một bức thư cho Keith Alexander, bày tỏ "sự biết ơn của ông và những lời chúc mừng vì sự hỗ trợ tình báo dấu hiệu nổi bật" mà Bộ Ngoại giao đã nhận được về Hội nghị thượng đỉnh lần thứ 5 của châu Mỹ, một hội nghị chuyên về thương thảo các thỏa thuận kinh tế. Trong thư, Shannon đặc biệt lưu ý rằng sự giám sát của NSA đã cung cấp cho Mỹ các ưu thế thương thảo vượt qua các bên khác:

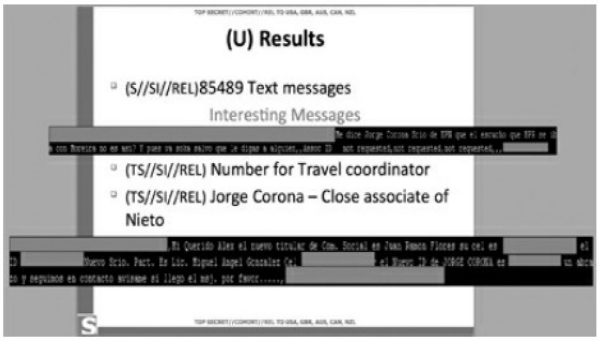


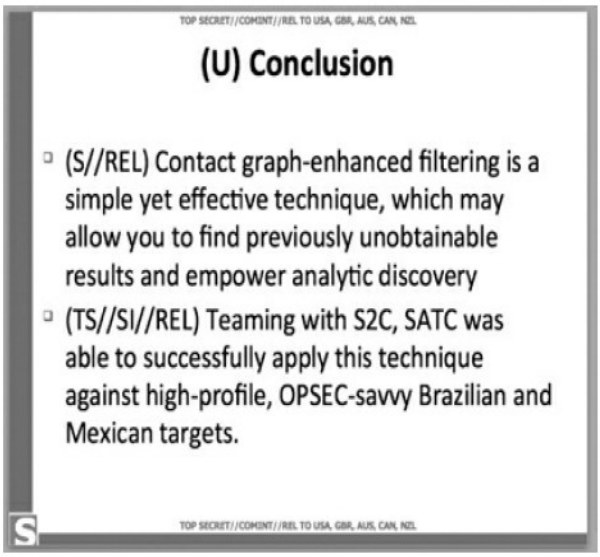
The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.

NSA dành ngang bằng với gián điệp ngoại giao, như các tài liệu tham chiếu tới "các công việc chính trị" thể hiện. Một ví dụ đặc biệt quá đáng, từ 2011, chỉ cách mà cơ quan này đã nhằm vào các nhà lãnh đạo Mỹ Latin - Dilma Rousseff, tổng thống Brazil, cùng với "các địch thủ chính của bà"; và Enrique Peña Nieto, sau này là ứng viên tổng thống hàng đầu của Mexico (và bây giờ là tổng thống), cùng với ""9 trong số các mối liên hệ gần gũi của ông" - vì sự "nổi lên" đối với sự giám sát đặc biệt tràn lan. Tài liệu thậm chí đặc trưng một số thông điệp văn bản bị can thiệp được Nieto gửi và nhận và một "mối quan hệ gần gũi":









Bạn có thể đoán vì sao các lãnh đạo chính trị của Brazil và Mexico từng là các mục tiêu của NSA.

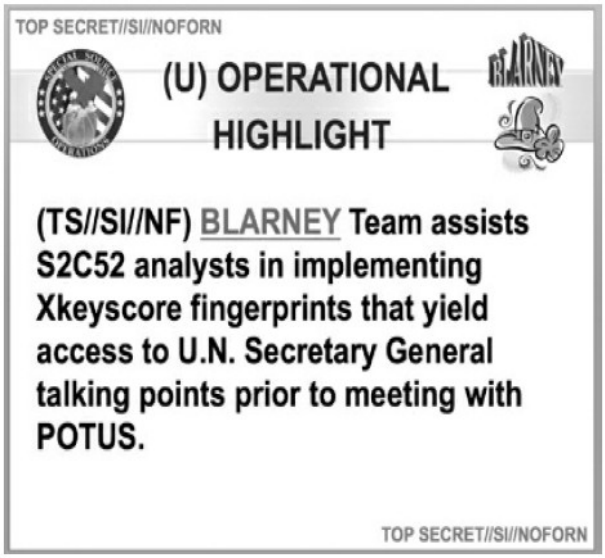
Cả 2 nước đều giàu tài nguyên dầu mỏ. Họ là sự hiện diện lớn và có ảnh hưởng trong khu vực. Và trong khi họ còn xa mới là các đối thủ, thì họ lại cũng không phải là các đồng minh gần gũi và tin cậy nhất của nước Mỹ. Quả thực, một tài liệu kế hoạch của NSA - có đầu đề "Nhận diện các thách thức: Các xu thế địa chính trị cho 2014-2019" - liệt kê cả Mexico và Brazil dưới đầu đề "Bạn bè, kẻ thù, hay vấn đề?" Các nước khác trong danh sách đó là Hy Lạp, Ấn Độ, Iran, Ả rập Xê út, Somalia, Sudan, Thổ Nhĩ Kỳ và Yemen.

Nhưng kết cục, trong trường hợp này như trong hầu hết các trường hợp khác, suy đoán về bất kỳ cái đích ngắm cụ thể nào cũng đều dựa vào một tiên đề sai. NSA không cần bất kỳ lý do đặc biệt hay hợp lý nào để can thiệp vào các giao tiếp truyền thông riêng tư của mọi người. Nhiệm vụ theo luật định của họ là thu thập mọi thứ.

Nếu là mọi thứ, thì những tiết lộ về việc NSA gián điệp các lãnh đạo nước ngoài là ít quan trọng hơn sự giám sát ồ ạt không có lệnh cho phép của cơ quan này đối với tất cả dân chúng. Các nước đã gián điệp các lãnh đạo nhà nước từ nhiều thế kỷ nay, bao gồm cả các đồng minh. Điều này là không đáng lưu ý, bất chấp sự la hét lớn đã xảy ra sau đó khi, ví dụ, thế giới đã phát hiện ra rằng NSA đã có nhiều năm nhằm vào điện thoại cầm tay của thủ tướng Đức Angela Merkel.

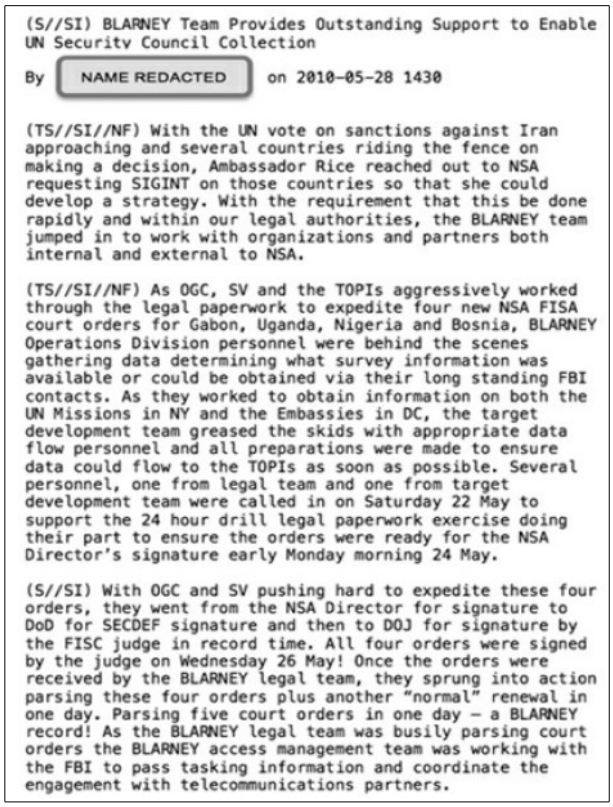
Đáng chú ý hơn là thực tế rằng hết nước này tới nước khác, các tiết lộ rằng NSA từng gián điệp hàng trăm triệu công dân của họ đã tạo ra nhiều hơn một chút những phản đối câm lặng từ lãnh đạo chính trị của họ. Sự căm phẫn thực sự đã phun ra hướng tới chỉ những lãnh đạo nào đã hiểu được rằng họ, và không chỉ các công dân của họ, cũng từng là đích ngắm.

Hơn nữa, phạm vi rộng lớn giám sát ngoại giao mà NSA đã trải nghiệm là bất thường và đáng chú ý. Bổ sung thêm tới các lãnh đạo nước ngoài, Mỹ, ví dụ, cũng đã gián điệp rộng khắp các tổ chức quốc tế như Liên hiệp quốc để giành được ưu thế ngoại giao. Một tóm tắt tháng 04/2013 từ SSO là điển hình, nêu cách mà cơ quan đó đã sử dụng các chương trình của mình để giành được các điểm nói chuyện của tổng thư ký Liên hiệp quốc trước cuộc gặp mặt của ông với Tổng thống Obama:



Vô số các tài liệu chi tiết hóa cách mà Susan Rice, sau này là đại sứ Liên hiệp quốc và bây giờ là cố

vấn an ninh quốc gia của Tổng thống Obama, đã yêu cầu lặp đi lặp lại rằng gián điệp của NSA trong các cuộc thảo luận nội bộ của các quốc gia thành viên chủ chốt để học các chiến lược thương thảo của họ. Một báo cáo của SSO vào tháng 05/2010 mô tả qui trình này trong mối liên kết với một nghị quyết đang được Liên hiệp quốc phác thảo có liên quan tới việc áp đặt trừng phạt mới lên Iran.



(S//SI) BLARNEY Team Provides Outstanding Support to Enable UN Security Council Collection

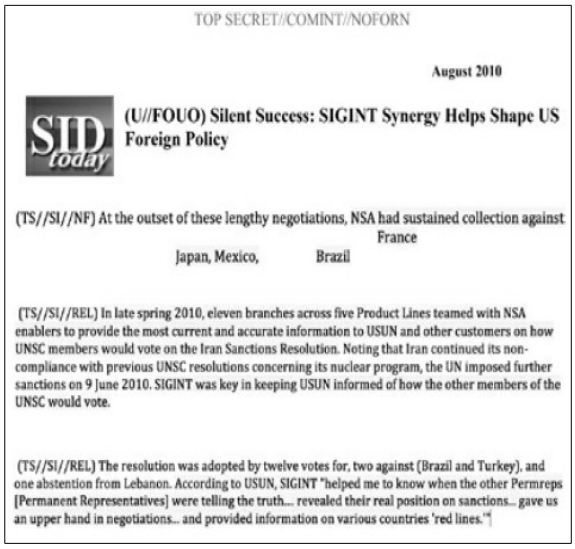
By NAME REDACTED on 2010-05-28 1430

(TS//SI//NF) With the UN vote on sanctions against Iran approaching and several countries riding the fence on making a decision, Ambassador Rice reached out to NSA requesting SIGINT on those countries so that she could develop a strategy. With the requirement that this be done rapidly and within our legal authorities, the BLARNEY team jumped in to work with organizations and partners both internal and external to NSA.

(TS//SI//NF) As OGC, SV and the TOPIs aggressively worked through the legal paperwork to expedite four new NSA FISA court orders for Gabon, Uganda, Nigeria and Bosnia, BLARNEY Operations Division personnel were behind the scenes gathering data determining what survey information was available or could be obtained via their long standing FBI contacts. As they worked to obtain information on both the UN Missions in NY and the Embassies in DC, the target development team greased the skids with appropriate data flow personnel and all preparations were made to ensure data could flow to the TOPIs as soon as possible. Several personnel, one from legal team and one from target development team were called in on Saturday 22 May to support the 24 hour drill legal paperwork exercise doing their part to ensure the orders were ready for the NSA Director's signature early Monday morning 24 May.

(S//SI) With OGC and SV pushing hard to expedite these four orders, they went from the NSA Director for signature to DoD for SECDEF signature and then to DOJ for signature by the FISC judge in record time. All four orders were signed by the judge on Wednesday 26 May! Once the orders were received by the BLARNEY legal team, they sprung into action parsing these four orders plus another "normal" renewal in one day. Parsing five court orders in one day – a BLARNEY record! As the BLARNEY legal team was busily parsing court orders the BLARNEY access management team was working with the FBI to pass tasking information and coordinate the engagement with telecommunications partners.

Một tài liệu giám sát tương tự từ tháng 08/2010 tiết lộ rằng Mỹ đã gián điệp 8 thành viên Hội đồng An ninh Liên hiệp quốc về nghị quyết sắp tới về các trừng phạt chống Iran. Danh sách đó bao gồm Pháp, Brazil, Nhật và Mexico - tất cả các quốc gia được cho là thân thiện. Vụ gián điệp đó đã trao cho chính phủ Mỹ thông tin quý giá về các ý định bỏ phiếu của các nước đó, trao cho Washington một cái lề khi nói chuyện với các thành viên khác của Hội đồng An ninh.



TOP SECRET//COMINT//NOFORN

August 2010

SID today

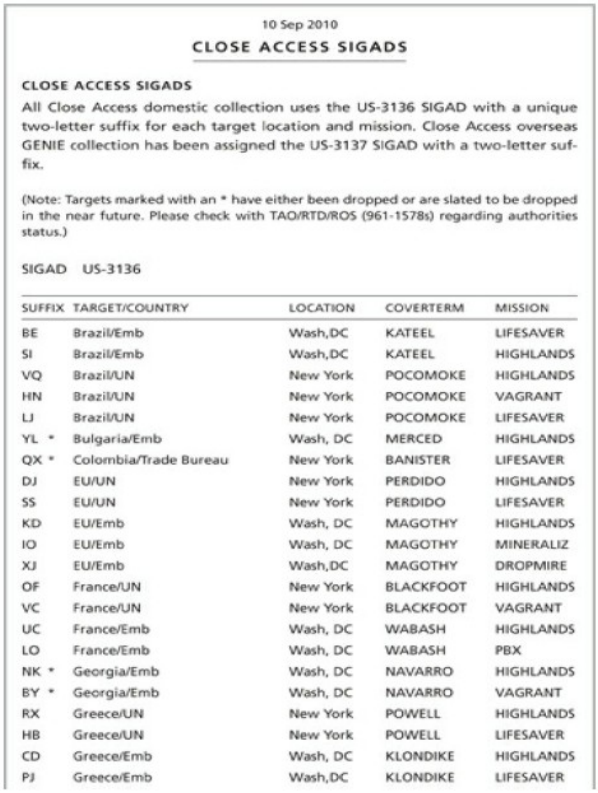
(U//FOUO) Silent Success: SIGINT Synergy Helps Shape US Foreign Policy

(TS//SI//NF) At the outset of these lengthy negotiations, NSA had sustained collection against France Japan, Mexico, Brazil

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) The resolution was adopted by twelve votes for, two against (Brazil and Turkey), and one abstention from Lebanon. According to USUN, SIGINT "helped me to know when the other Permreps [Permanent Representatives] were telling the truth... revealed their real position on sanctions... gave us an upper hand in negotiations... and provided information on various countries 'red lines.'"

Để tạo thuận lợi cho việc gián điệp ngoại giao, NSA đã giành được các dạng truy cập khác nhau tới các sứ quán và lãnh sự quán của nhiều nước đồng minh thân cận nhất. Một tài liệu năm 2010 - chỉ ra ở đây với một số nước bị xóa - liệt kê các nước mà các cấu trúc ngoại giao của họ ở trong nước Mỹ từng bị cơ quan này thâm nhập. Một bảng chú giải ở cuối giải thích các dạng giám sát khác nhau được sử dụng.



10 Sep 2010

CLOSE ACCESS SIGADS

CLOSE ACCESS SIGADS

All Close Access domestic collection uses the US-3136 SIGAD with a unique two-letter suffix for each target location and mission. Close Access overseas GENIE collection has been assigned the US-3137 SIGAD with a two-letter suffix.

(Note: Targets marked with an * have either been dropped or are slated to be dropped in the near future. Please check with TAO/RTD/ROS (961-1578s) regarding authorities status.)

SIGAD US-3136

SUFFIX	TARGET/COUNTRY	LOCATION	COVERTERM	MISSION
BE	Brazil/Emb	Wash,DC	KATEEL	LIFESAVER
SI	Brazil/Emb	Wash,DC	KATEEL	HIGHLANDS
VQ	Brazil/UN	New York	POCOMOKE	HIGHLANDS
HN	Brazil/UN	New York	POCOMOKE	VAGRANT
LJ	Brazil/UN	New York	POCOMOKE	LIFESAVER
YL *	Bulgaria/Emb	Wash, DC	MERCED	HIGHLANDS
QX *	Colombia/Trade Bureau	New York	BANISTER	LIFESAVER
DJ	EU/UN	New York	PERDIDO	HIGHLANDS
SS	EU/UN	New York	PERDIDO	LIFESAVER
KD	EU/Emb	Wash, DC	MAGOTHY	HIGHLANDS
IO	EU/Emb	Wash, DC	MAGOTHY	MINERALIZ
XJ	EU/Emb	Wash,DC	MAGOTHY	DROPMIRE
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX
NK *	Georgia/Emb	Wash, DC	NAVARRO	HIGHLANDS
BY *	Georgia/Emb	Wash, DC	NAVARRO	VAGRANT
RX	Greece/UN	New York	POWELL	HIGHLANDS
HB	Greece/UN	New York	POWELL	LIFESAVER
CD	Greece/Emb	Wash, DC	KLONDIKE	HIGHLANDS
PJ	Greece/Emb	Wash,DC	KLONDIKE	LIFESAVER

JN	Greece/Emb	Wash, DC	KLONDIKE	PBX
MO *	India/UN	New York	NASHUA	HIGHLANDS
QL *	India/UN	New York	NASHUA	MAGNETIC
ON *	India/UN	New York	NASHUA	VAGRANT
IS *	India/UN	New York	NASHUA	LIFESAVER
OX *	India/Emb	Wash,DC	OSAGE	LIFESAVER
CQ *	India/Emb	Wash, DC	OSAGE	HIGHLANDS
TQ *	India/Emb	Wash, DC	OSAGE	VAGRANT
CU *	India/EmbAnx	Wash, DC	OSWAYO	VAGRANT
DS *	India/EmbAnx	Wash, DC	OSWAYO	HIGHLANDS
SU *	Italy/Emb	Wash, DC	BRUNEAU	LIFESAVER
MV *	Italy/Emb	Wash, DC	HEMLOCK	HIGHLANDS
IP *	Japan/UN	New York	MULBERRY	MINERALIZ
HF *	Japan/UN	New York	MULBERRY	HIGHLANDS
BT *	Japan/UN	New York	MULBERRY	MAGNETIC
RU *	Japan/UN	New York	MULBERRY	VAGRANT
LM *	Mexico/UN	New York	ALAMITO	LIFESAVER
UX *	Slovakia/Emb	Wash, DC	FLEMING	HIGHLANDS
SA *	Slovakia/Emb	Wash, DC	FLEMING	VAGRANT
XR *	South Africa/ UN & Consulate	New York	DOBIE	HIGHLANDS
RJ *	South Africa/ UN & Consulate	New York	DOBIE	VAGRANT
YR *	South Korea/UN	New York	SULPHUR	VAGRANT
TZ *	Taiwan/TECO	New York	REQUETTE	VAGRANT
VN *	Venezuela/Emb	Wash, DC	YUKON	LIFESAVER
UR *	Venezuela/UN	New York	WESTPORT	LIFESAVER
NO *	Vietnam/UN	New York	NAVAJO	HIGHLANDS
OU *	Vietnam/UN	New York	NAVAJO	VAGRANT
GV *	Vietnam/Emb	Wash, DC	PANTHER	HIGHLANDS

SIGAD US-3137

GENERAL TERM DESCRIPTIONS

HIGHLANDS: Collection from Implants
VAGRANT: Collection of Computer Screens
MAGNETIC: Sensor Collection of Magnetic Emanations
MINERALIZE: Collection from LAN Implant
OCEAN: Optical Collection System for Raster-Based Computer Screens

LIFESAVER: Imaging of the Hard Drive
GENIE: Multi-stage operation; jumping the airgap etc.
BLACKHEART: Collection from an FBI Implant
PBX: Public Branch Exchange Switch
CRYPTO ENABLED: Collection derived from AO's efforts to enable crypto
DROPMIRE: passive collection of emanations using an antenna
CUSTOMS: Customs opportunities (not LIFESAVER)
DROPMIRE: Laser printer collection, purely proximal access (**NOT** implanted)
DEWSWEEPER: USB (Universal Serial Bus) hardware host tap that provides COVERT link over USB link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network.
RADON: Bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-directional exploitation of Denied networks using standard on-net tools.

Một số phương pháp của NSA phục vụ cho tất cả các chương trình nghị sự - kinh tế, ngoại giao, an ninh và giành được một ưu thế toàn cầu cho tất cả các mục đích - và chúng là trong số các phương pháp tràn lan, đạo đức giả nhất, trong kho các tiết mục của cơ quan này. Nhiều năm, chính phủ Mỹ đã to tiếng cảnh báo thế giới rằng các bộ định tuyến routers của Trung Quốc và các thiết bị Internet khác đặt ra một "mối đe dọa" vì chúng được xây dựng với chức năng giám sát cửa hậu mà trao cho chính phủ Trung Quốc khả năng gián điệp bất kỳ ai đang sử dụng chúng. Vâng những gì các tài liệu của NSA chỉ ra rằng những người Mỹ đã và đang tham gia chính xác trong các hoạt động mà nước Mỹ đã tố cáo Trung Quốc đang làm.

Sự khua trống của những lời tố cáo của Mỹ chống các nhà sản xuất thiết bị Internet của Trung Quốc từng không thuyên giảm. Vào năm 2012, ví dụ, một báo cáo từ Ủy ban Tình báo Hạ viện, do Mike Rogers lãnh đạo, đã kêu rằng Hoa Vĩ (Huawei) và ZTE, 2 công ty thiết bị viễn thông hàng đầu của Trung Quốc, "có thể đang vi phạm các luật của Mỹ" và đã "không tuân thủ các bổn phận pháp lý hoặc các tiêu chuẩn quốc tế về hành xử của doanh nghiệp". Ủy ban đó đã khuyến cáo rằng "Mỹ nên xem xét với sự nghi ngờ về sự thâm nhập liên tục của các công ty viễn thông Trung Quốc vào thị trường viễn thông Mỹ".

Ủy ban của Rogers đã lên tiếng về các nỗi sợ hãi rằng 2 công ty đó từng xúc tác cho sự giám sát của nhà nước Trung Quốc, dù nó đã nhận thức được rằng nó đã không có được bằng chứng thực sự nào rằng các hãng đó đã cài cắm vào các bộ định tuyến router và các hệ thống khác của họ với các thiết bị giám sát. Tuy nhiên, nó đã trích dẫn sự thất bại của các công ty đó để hợp tác và đã thúc giục các hãng Mỹ tránh mua các sản phẩm của họ:

> Các thực thể khu vực tư nhân ở Mỹ được khuyến khích mạnh mẽ cân nhắc các rủi ro dài hạn về an ninh có liên quan tới việc tiến hành kinh doanh với hoặc ZTE hoặc Hoa Vĩ về trang thiết bị hoặc các dịch vụ. Các nhà cung cấp mạng và các lập trình viên hệ thống của Mỹ được khuyến cáo mạnh mẽ tìm kiếm các nhà bán hàng khác cho các dự án của họ. Dựa vào các thông tin mật và không mật đang có sẵn, Hoa Vĩ và ZTE không thể được tin cậy sẽ có tự do đối với ảnh hưởng của nước ngoài và vì thế đặt ra một mối đe dọa về an ninh cho nước Mỹ và cho các hệ thống của họ.

Những tố cáo liên tục đã trở thành một gánh nặng như vậy nên Ren Zhengfei, nhà sáng lập và CEO 69 tuổi của Hoa Vĩ, đã công bố hồi tháng 11/2013 rằng hãng đã bỏ thị trường Mỹ. Như tờ *Chính sách Nước ngoài* đã nêu, Zhengfei đã nói cho một tờ báo Pháp: "'Nếu Hoa Vĩ đang nằm ở giữa các mối quan hệ Mỹ - Trung', thì sự gây ra các vấn đề, 'là không đáng'".

Nhưng trong khi các công ty Mỹ từng được cảnh báo tránh xa các bộ định tuyến router được cho là không đáng tin cậy của Trung Quốc, thì các tổ chức nước ngoài có thể được tư vấn tốt để nhận biết được các bộ định tuyến router do Mỹ chế tạo. Một báo cáo tháng 06/2010 từ người đứng đầu phòng Phát triển đích và Truy cập của NSA lại bị sốc một cách rõ ràng. NSA thường xuyên nhận - hoặc can thiệp - các bộ định tuyến router, các máy chủ và các thiết bị mạng máy tính khác đang được xuất khẩu từ Mỹ trước khi chúng được phân phối tới các khách hàng quốc tế. Cơ quan này sau đó cài cắm các công cụ giám sát cửa hậu, đóng gói lại các thiết bị với một dấu triện của xưởng sản xuất, và gửi chúng đi. NSA vì thế giành được sự truy cập tới toàn bộ các mạng và tất cả những người sử dụng của họ. Tài liệu hân hoan quan sát thấy rằng một số "chế phẩm SIGINT ... là rất thực tiễn (theo nghĩa đen!)":

TOP SECRET//COMINT//NOFORN

June 2010

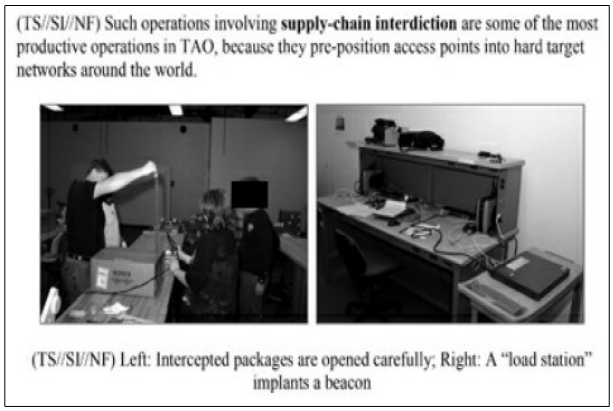
SID today

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) [NAME REDACTED], Chief, Access and Target Development (S3261)

IMAGE REDACTED

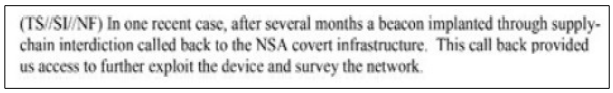
(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.



(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

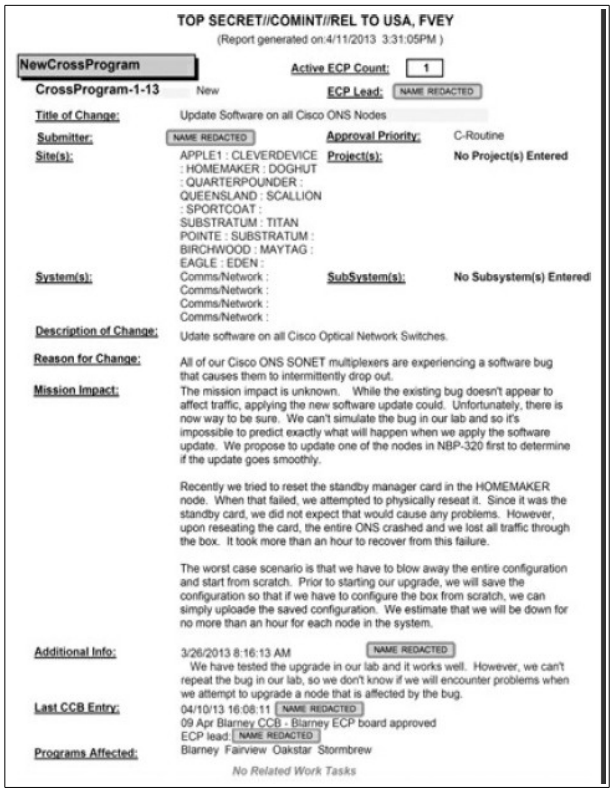
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Cuối cùng, thiết bị được cài cắm đó kết nối ngược về hạ tầng của NSA:



(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.

Trong số những thiết bị khác, cơ quan này can thiệp và làm giả với các bộ định tuyến router và các máy chủ được Cisco sản xuất để định hướng số lượng lớn các giao thông Internet ngược về các kho của NSA. (Không có bằng chứng trong các tài liệu rằng Cisco biết được, hoặc tha thứ, cho các can thiệp đó). Vào tháng 04/2013, cơ quan này đã níu lấy các khó khăn kỹ thuật có liên quan tới các bộ chuyển mạch mạng Cisco bị can thiệp, chúng đã ảnh hưởng tới các chương trình BLARNEY, FAIRVIEW, OAKSTAR, và STORMBREW:



TOP SECRET//COMINT//REL TO USA, FVEY

(Report generated on:4/11/2013 3:31:05PM)

NewCrossProgram — Active ECP Count: 1

CrossProgram-1-13 New — ECP Lead: [NAME REDACTED]

Title of Change: Update Software on all Cisco ONS Nodes

Submitter: [NAME REDACTED] — Approval Priority: C-Routine

Site(s): APPLE1 : CLEVERDEVICE : HOMEMAKER : DOGHUT : QUARTERPOUNDER : QUEENSLAND : SCALLION : SPORTCOAT : SUBSTRATUM : TITAN POINTE : SUBSTRATUM : BIRCHWOOD : MAYTAG : EAGLE : EDEN : — Project(s): No Project(s) Entered

System(s): Comms/Network : Comms/Network : Comms/Network : Comms/Network : — SubSystem(s): No Subsystem(s) Entered

Description of Change: Udate software on all Cisco Optical Network Switches.

Reason for Change: All of our Cisco ONS SONET multiplexers are experiencing a software bug that causes them to intermittently drop out.

Mission Impact: The mission impact is unknown. While the existing bug doesn't appear to affect traffic, applying the new software update could. Unfortunately, there is now way to be sure. We can't simulate the bug in our lab and so it's impossible to predict exactly what will happen when we apply the software update. We propose to update one of the nodes in NBP-320 first to determine if the update goes smoothly.

Recently we tried to reset the standby manager card in the HOMEMAKER node. When that failed, we attempted to physically reseat it. Since it was the standby card, we did not expect that would cause any problems. However, upon reseating the card, the entire ONS crashed and we lost all traffic through the box. It took more than an hour to recover from this failure.

The worst case scenario is that we have to blow away the entire configuration and start from scratch. Prior to starting our upgrade, we will save the configuration so that if we have to configure the box from scratch, we can simply uploade the saved configuration. We estimate that we will be down for no more than an hour for each node in the system.

Additional Info: 3/26/2013 8:16:13 AM [NAME REDACTED]
We have tested the upgrade in our lab and it works well. However, we can't repeat the bug in our lab, so we don't know if we will encounter problems when we attempt to upgrade a node that is affected by the bug.

Last CCB Entry: 04/10/13 16:08:11 [NAME REDACTED]
09 Apr Blarney CCB - Blarney ECP board approved
ECP lead: [NAME REDACTED]

Programs Affected: Blarney Fairview Oakstar Stormbrew

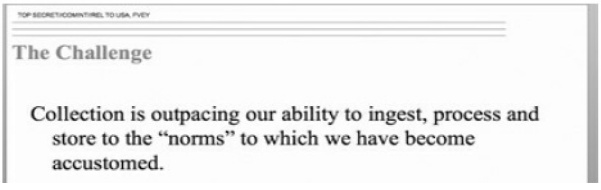
No Related Work Tasks

Hoàn toàn có khả năng rằng các hãng của Trung Quốc đang cài cắm các cơ chế giám sát trong các thiết bị mạng của họ. Nhưng nước Mỹ chắc chắn cũng đang làm y hệt.

Cảnh báo cho thế giới về sự giám sát của Trung Quốc có thể từng là một trong những động lực đằng sau những khiếu nại của chính phủ Mỹ rằng các thiết bị của Trung Quốc không thể tin cậy được. Nhưng một động lực quan trọng ngang bằng dường như đã và đang ngăn chặn các thiết bị của Trung Quốc khỏi hất cẳng được các thiết bị được Mỹ sản xuất, điều có thể đã giới hạn sự vươn tới được của chính NSA. Nói cách khác, các bộ định tuyến router và các máy chủ Trung Quốc đại diện cho không chỉ sự cạnh tranh về kinh tế, mà còn sự cạnh tranh về giám sát: khi ai đó mua một thiết bị của Trung Quốc thay vì của Mỹ, thì NSA đánh mất phương tiện cốt tử để gián điệp nhiều hơn các hoạt động giao tiếp truyền thống.

***

Nếu lượng thu thập được phát hiện đã làm cho u muội đi rồi, thì nhiệm vụ của NSA để thu thập tất cả các dấu hiệu mọi lúc đã dẫn cơ quan này tới mở rộng và xâm chiếm ngày càng nhiều miền đất hơn. Lượng các dữ liệu mà nó chộp được là quá khổng lồ, trong thực tế, thách thức cơ bản mà cơ quan này nêu là về việc lưu trữ hàng đống thông tin được tích cóp từ khắp nơi trên thế giới. Một tài liệu của NSA, được chuẩn bị cho Hội nghị SigDev của 5 cặp mắt, đưa ra vấn đề trọng tâm này:

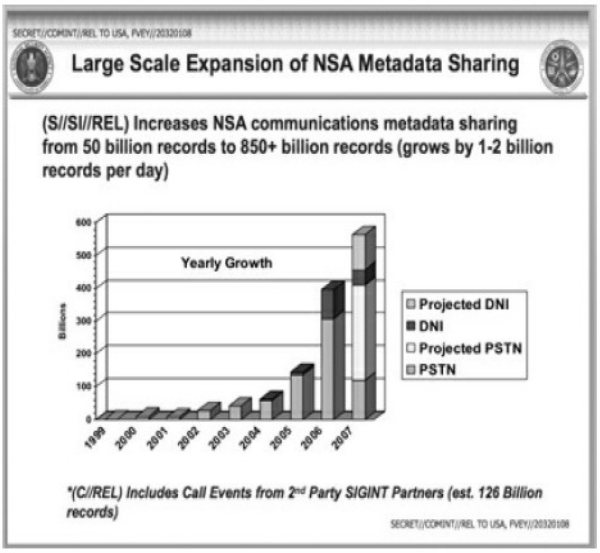


TOP SECRET//COMINT//REL TO USA, FVEY

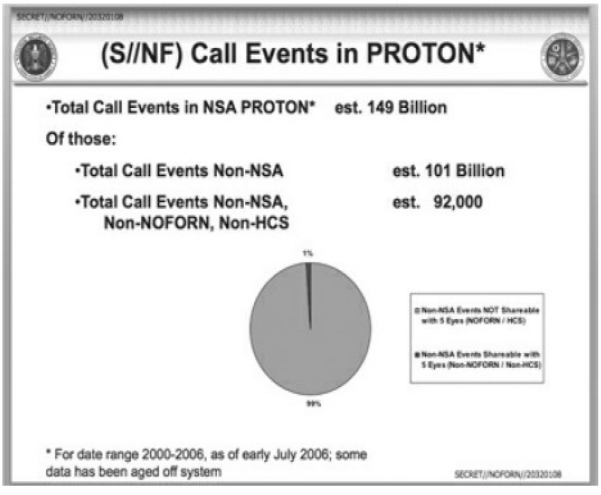
The Challenge

Collection is outpacing our ability to ingest, process and store to the "norms" to which we have become accustomed.

Câu chuyện đi ngược về năm 2006, khi cơ quan này nhảy lên cái gọi là "Sự mở rộng Phạm vi Rộng của việc Chia sẻ Siêu dữ liệu của NSA" (Large Scale Expansion of NSA Metadata Sharing). Tại thời điểm đó, NSA đã đoán trước được rằng sự thu thập siêu dữ liệu của nó có thể tăng tới 600 tỷ bản ghi mỗi năm, sự gia tăng có thể bao gồm từ 1-2 tỷ sự kiện cuộc gọi điện thoại mới được thu thập mỗi ngày:



Tới tháng 05/2007, sự mở rộng đó thực sự đã đơm hoa kết trái: lượng siêu dữ liệu điện thoại mà cơ quan này từng lưu trữ - độc lập với các dữ liệu thư điện tử và Internet khác, và không tính tới các dữ liệu mà NSA đã xóa vì thiếu chỗ lưu trữ - đã tăng tới 150 tỷ bản ghi:



Một khi các giao tiếp truyền thông dựa vào Internet đã được thêm vào sự pha trộn, tổng số các sự kiện giao tiếp truyền thông được lưu trữ từng là gần 1.000 tỷ (dữ liệu này, nó sẽ được lưu ý tới, sau đó được NSA chia sẻ với các cơ quan khác).

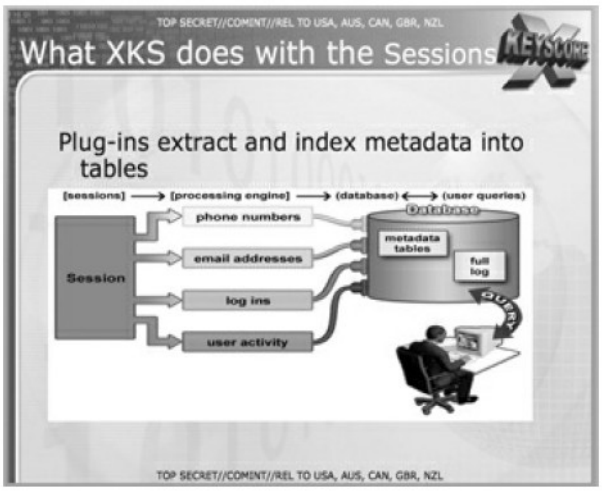
Để giải quyết vấn đề lưu trữ của nó, NSA đã bắt đầu xây dựng một cơ sở mới khổng lồ ở Bluffdale,

Utah, mà có một trong những mục đích ban đầu của nó để giữ lại tất cả các dữ liệu. Như nhà báo James Bamford đã lưu ý trong năm 2012, xây dựng Bluffdale sẽ mở rộng khả năng của cơ quan này bằng việc bổ sung thêm "4 khoảng diện tích 25.000 foot vuông được điền đầy với các máy chủ, đầy đủ với không gian mặt sàn được nâng cao lên cho các cáp và kho lưu trữ. Hơn nữa, sẽ có nhiều hơn 900.000 foot vuông dành cho hỗ trợ kỹ thuật và hành chính". Xem xét kích cỡ của tòa nhà và thực tế là, như Bamford nói, "một terabyte dữ liệu bây giờ có thể được lưu trữ trong một đĩa flash kích cỡ ngón tay út của một người", thì những ngụ ý về thu thập dữ liệu là sâu thẳm.

Nhu cầu về các cơ sở lớn hơn chưa từng có là đặc biệt cấp bách biết rằng những xâm lấn hiện hành trong hoạt động trực tuyến toàn cầu được mở rộng vượt xa sự thu thập siêu dữ liệu để bao gồm cả nội dung thực tế của các thư điện tử, duyệt Web, lịch sử tìm kiếm và các cuộc chat. Chương trình chính được NSA sử dụng để thu thập và tìm kiếm các dữ liệu như vậy, được giới thiệu vào năm 2007, là X-KEYSCORE, và nó đủ sức cho một bước nhảy căn bản trong phạm vi sức mạnh giám sát của cơ quan này. NSA gọi hệ thống "mở rộng mềm dẻo" của nó là X-KEYSCORE cho việc thu thập các dữ liệu điện tử, và với lý do tốt.

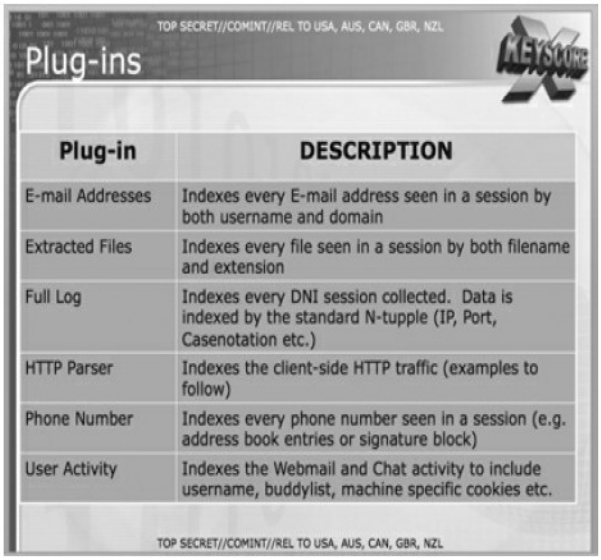
Một tài liệu huấn luyện được chuẩn bị cho các nhà phân tích nêu chương trình lấy được "gần như mọi điều mà một người sử dụng điển hình làm trên Internet", bao gồm cả văn bản của các thư điện tử, các tìm kiếm của Google, và các tên website được viếng thăm. X-KEYSCORE thậm chí cho phép NSA quan sát các hoạt động thư điện tử và duyệt khi chúng diễn ra.

Ngoài việc thu thập các dữ liệu toàn diện về các hoạt động trực tuyến của hàng trăm triệu người, X-KEYSCORE còn cho phép bất kỳ nhà phân tích nào của NSA tìm kiếm các cơ sở dữ liệu của hệ thống theo địa chỉ thư điện tử, số điện thoại, hoặc việc nhận diện các thuộc tính như một địa chỉ IP. Dải các thông tin sẵn sàng và cơ bản có nghĩa là một nhà phân tích sử dụng để tìm kiếm nó sẽ được miêu tả trong slide này:

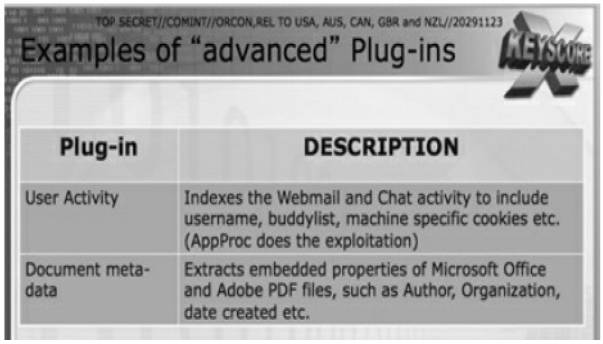


Một slide khác về X-KEYSCORE liệt kê các trường thông tin khác nhau mà có thể được tìm kiếm thông qua các "trình cài cắm" (plug-ins) của chương trình. Chúng bao gồm "mọi địa chỉ thư điện tử trong một phiên", "mọi số điện thoại được thấy trong một phiên" (bao gồm cả "các khoản mục của

sổ địa chỉ"), và "hoạt động của webmail và chat":

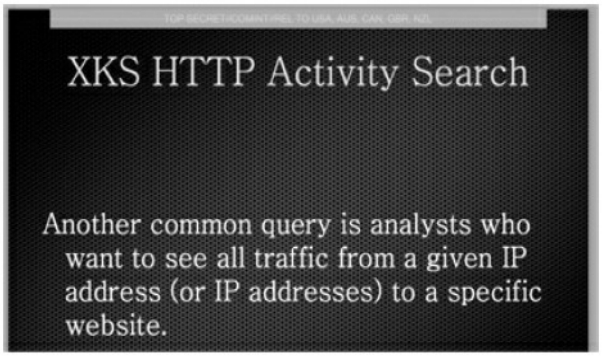


Chương trình cũng đưa ra khả năng tìm kiếm và truy xuất các tài liệu nhúng và các hình ảnh đã được tạo ra, gửi đi hoặc nhận được:



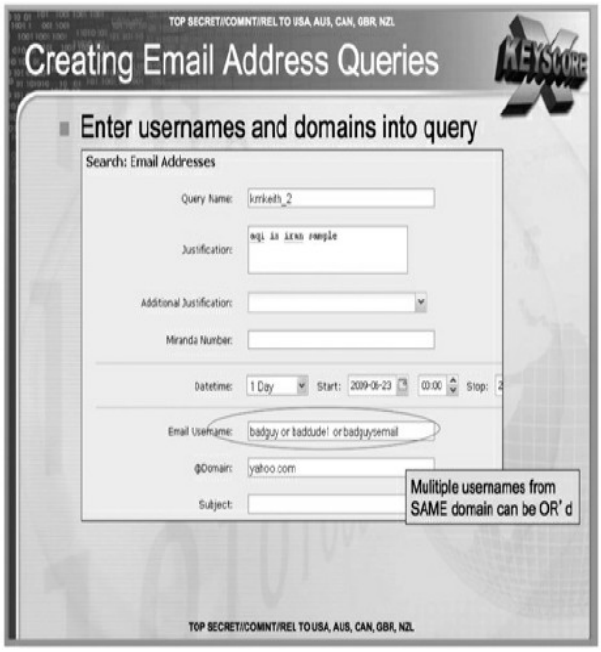
Các slide khác của NSA công bố cởi mở chứa đựng tất cả tham vọng toàn cầu của X-KEYSCORE:

Các tìm kiếm được chương trình xúc tác là quá đặc thù mà bất kỳ nhà phân tích nào của NSA cũng có khả năng không chỉ tìm ra các website nào một người đã viếng thăm mà còn tập hợp một danh sách toàn diện của tất cả các cuộc viếng thăm tới một website cụ thể nào đó từ các máy tính được chỉ định:



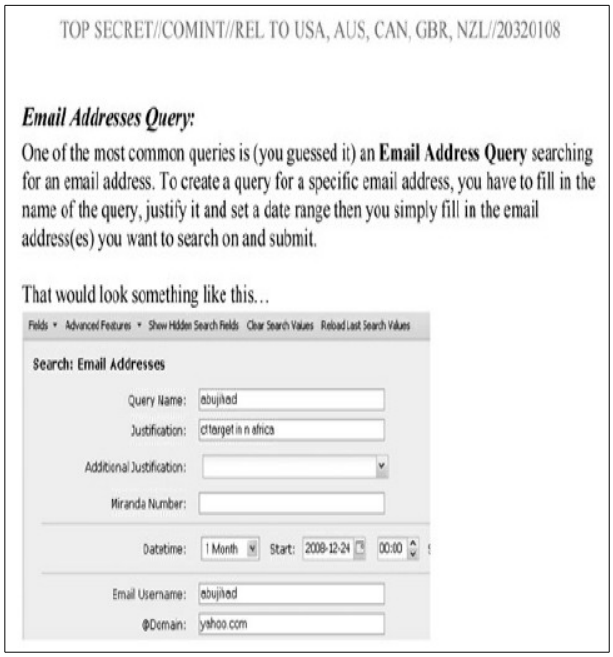
Đáng lưu ý nhất là sự dễ dàng mà các nhà phân tích có thể tìm kiếm bất kỳ điều gì họ muốn mà không có sự giám quản nào. Một nhà phân tích với sự truy cập tới X-KEYSCORE cần không đệ trình một yêu cầu tới một người giám sát hoặc bất kỳ nhà chức trách nào khác. Thay vào đó, nhà phân tích đơn giản điền vào một mẫu cơ bản để "xác minh" sự giám sát, và hệ thống trả về thông tin

được yêu cầu.

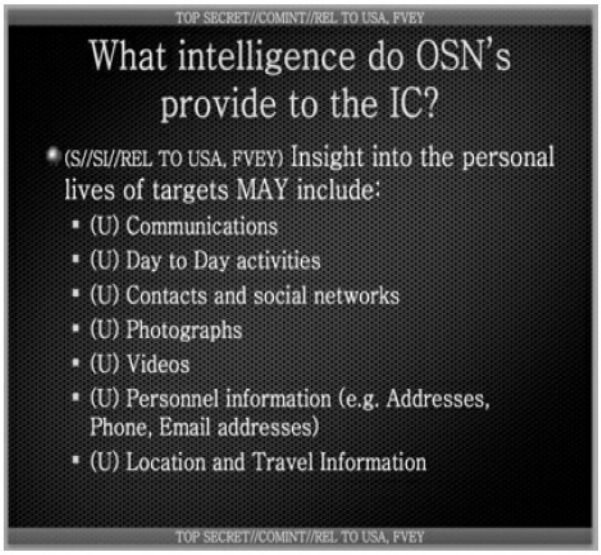


Trong cuộc phỏng vấn trên video đầu tiên mà anh ta đã đưa ra khi còn ở Hong Kong, Edward Snowden đã thực hiện một tuyên bố bạo gan: "Tôi, đang ngồi ở bàn của tôi, có thể nghe trộm điện thoại của bất kỳ ai, từ bạn hoặc kế toán viên của bạn, tới một thẩm phán liên bang hoặc thậm chí tổng thống, nếu tôi đã có được một thư điện tử cá nhân". Các quan chức Mỹ đã cực lực từ chối rằng điều này là đúng. Mike Rogers rõ ràng đã tố cáo Snowden "nói dối", bổ sung thêm, "Không có khả năng cho anh ta để làm những gì anh ta vừa nói anh ta có thể". Nhưng X-KEYSCORE cho phép một nhà phân tích làm chính xác những gì Snowden đã nói: ngắm đích bất kỳ người sử dụng nào cho việc giám sát toàn diện, bao gồm việc đọc nội dung các thư điện tử của họ. Quả thực, chương trình đó để lại cho một nhà phân tích tìm kiếm tất cả các thư điện tử mà bao gồm những người sử dụng bị ngắm đích ở dòng "CC" hoặc nhớ tới họ trong thân của văn bản.

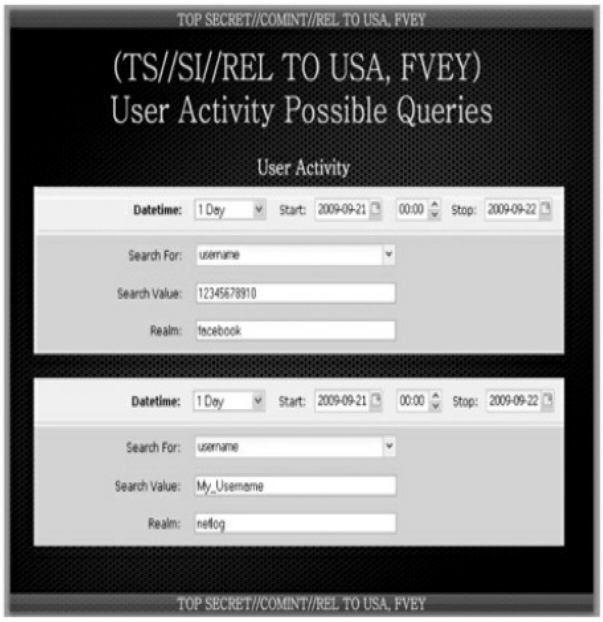
Các mệnh lệnh của riêng NSA cho việc tìm kiếm qua các thư điện tử chỉ thể hiện cách thức đơn giản đối với các nhà phân tích để giám sát bất kỳ ai mà họ biết được địa chỉ của những người đó:



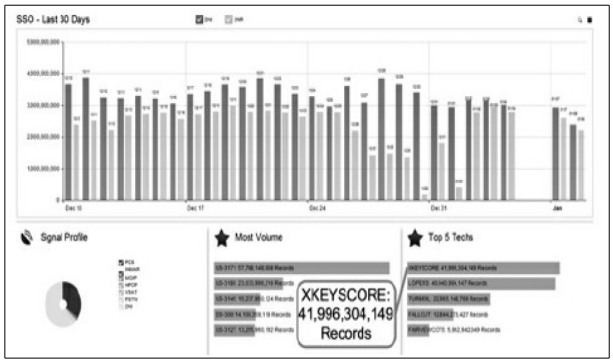
Một trong các chức năng có giá trị nhất của X-KEYSCORE đối với NSA là khả năng của nó để giám sát các hoạt động trong các mạng xã hội trực tuyến - OSN (Online Social Network), như Facebook và Twitter, mà cơ quan này tin tưởng đưa ra một sự giàu có các thông tin và "sự hiểu thấu trong cuộc sống của các cá nhân bị ngắm đích".



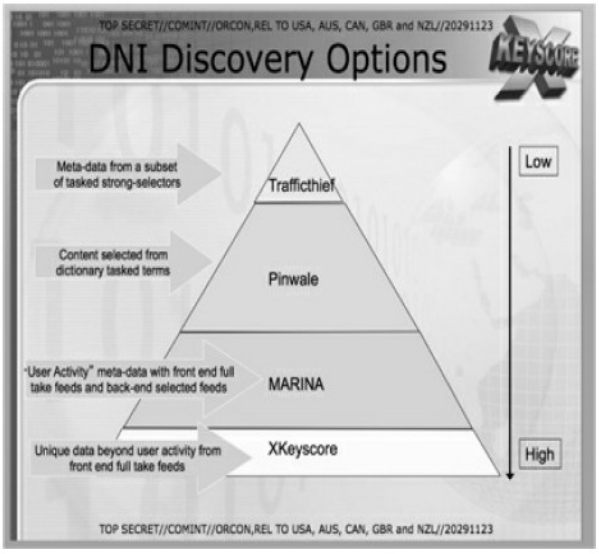
Các phương pháp cho việc tìm kiếm các hoạt động phương tiện xã hội là đơn giản từng bit như tìm kiếm thư điện tử. Một nhà phân tích nhập vào Facebook tên người sử dụng mong muốn, cùng với dải các dữ liệu về hoạt động, và X-KEYSCORE sau đó trả về tất cả thông tin của người sử dụng đó, bao gồm cả các thông điệp, nội dung các cuộc chat, và các thông tin riêng tư khác.



Có lẽ thực tế đáng chú ý nhất về X-KEYSCORE là số lượng khổng lồ các dữ liệu mà nó lấy được và lưu trữ trong nhiều site thu thập khắp thế giới. "Ở một số site", một báo cáo nêu, "lượng dữ liệu chúng tôi nhận được mỗi ngày (hơn 20 terabyte) chỉ có thể được lưu trữ ít hơn 24 giờ dựa vào các tài nguyên có sẵn". Đối với một giai đoạn 30 ngày bắt đầu trong tháng 12/2012, lượng các bản ghi được X-KEYSCORE thu thập chỉ cho một đơn vị, SSO, đã vượt quá 41 tỷ:



X-KEYSCORE "lưu trữ đầy đủ nội dung lấy được cho 3-5 ngày, 'làm chậm đi Internet' một cách có hiệu lực" - nghĩa là "các nhà phân tích có thể đi ngược về và phục hồi lại các phiên làm việc". Sau đó "nội dung nào mà 'thú vị' có thể được kéo ra khỏi X-KEYSCORE và được đẩy vào Agility hoặc PINWALE", các cơ sở dữ liệu lưu trữ mà được giữ lại lâu hơn.



Khả năng của X-KEYSCORE để truy cập Facebook và các site phương tiện xã hội khác được các chương trình khác khoe khoang, bao gồm BLARNEY, cho phép NSA theo dõi "một dải rộng lớn các dữ liệu của Facebook thông qua các hoạt động giám sát và tìm kiếm":

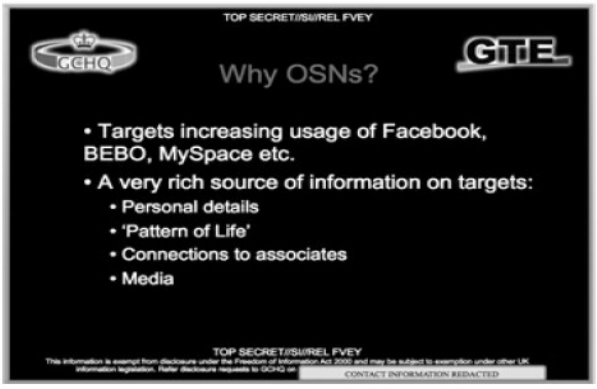
(TS//SI//NF) BLARNEY Exploits the Social Network via Expanded Facebook Collection

By [NAME REDACTED] on 2011-03-14 0737

(TS//SI//NF) SSO HIGHLIGHT - BLARNEY Exploits the Social Network via Expanded Facebook Collection

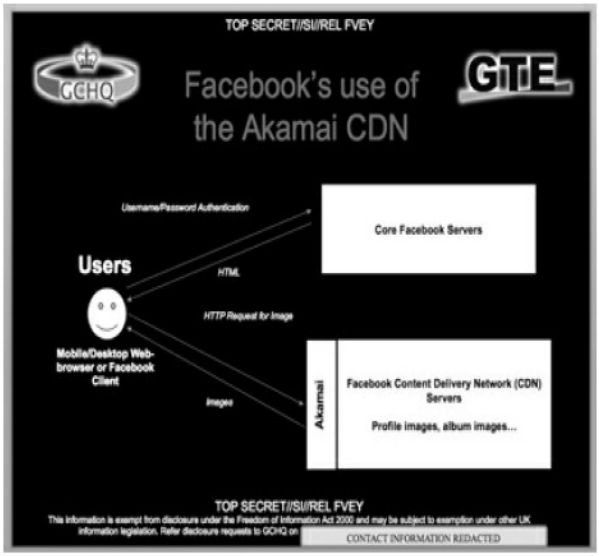
(TS//SI//NF) On 11 March 2011, BLARNEY began delivery of substantially improved and more complete Facebook content. This is a major leap forward in NSA's ability to exploit Facebook using FISA and FAA authorities. This effort was initiated in partnership with the FBI six months ago to address an unreliable and incomplete Facebook collection system. NSA is now able to access a broad range of Facebook data via surveillance and search activities. OPIs are excited about receiving many content fields, such as chat, on a sustained basis that had previously only been occasionally available. Some content will be completely new including subscriber videos. Taken together, the new Facebook collection will provide a robust SIGINT opportunity against our targets – from geolocation based on their IP addresses and user agent, to collection of all of their private messages and profile information. Multiple elements across NSA partnered to ensure the successful delivery of this data. An NSA representative at FBI coordinated the rapid development of the collection system; SSO's PRINTAURA team wrote new software and made configuration changes; CES modified their protocol exploitation systems and the Technology Directorate fast-tracked upgrades to their data presentation tools so that OPIs could view the data properly.

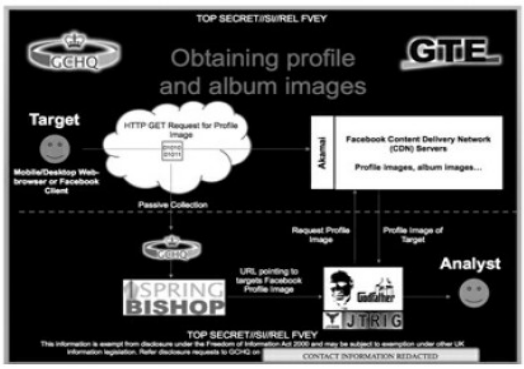
Trong khi đó tại Anh, bộ phận Khai thác Viễn thông Toàn cầu - GTE (Global Telecommunications Exploitation) của GCHQ cũng đã dành các tài nguyên đáng kể vào nhiệm vụ đó, được chi tiết hóa trong một trình chiếu năm 2011 cho hội nghị thường niên của 5 cặp mắt.



GCHQ đã chú ý đặc biệt tới những điểm yếu trong hệ thống an ninh của Facebook và thu được dạng các dữ liệu mà những người sử dụng Facebook định bảo vệ:

Đặc biệt, GCHQ đã thấy các chỗ bị tổn thương trong hệ thống mạng lưu trữ ảnh, nó có thể được sử dụng để có được sự truy cập tới các mã định danh ID của Facebook và các ảnh trong các bộ ảnh:





Ngoài các mạng phương tiện xã hội, NSA và GCHQ tiếp tục tìm kiếm bất kỳ khe hở nào trong mạng giám sát của họ, bất kỳ giao tiếp truyền thông nào còn nằm bên ngoài sự chộp được của họ, và sau đó phát triển các cách thức để mang chúng vào dưới các con mắt theo dõi của các cơ quan đó. Một chương trình dường như tù mù mô tả điểm này.

Cả NSA và GCHQ đã từng tiêu thụ theo nhu cầu lĩnh hội được của họ để theo dõi các giao tiếp

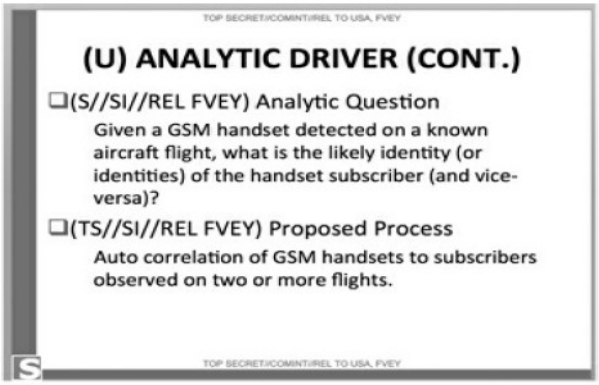
truyền thông Internet và điện thoại của mọi người trên các chuyến bay thương mại. Vì chúng được định tuyến thông qua các hệ thống vệ tinh độc lập, chúng là cực kỳ khó để định vị. Ý tưởng là có một thời điểm khi mà ai đó có thể sử dụng Internet hoặc điện thoại của họ mà không có sự dò tìm ra - thậm chí chỉ trong ít giờ đồng hồ trong khi bay - là không chịu đựng được đối với các cơ quan giám sát. Để đáp lại, họ đã dành các tài nguyên đáng kể cho việc phát triển các hệ thống sẽ can thiệp được các giao tiếp truyền thông trong khi bay.

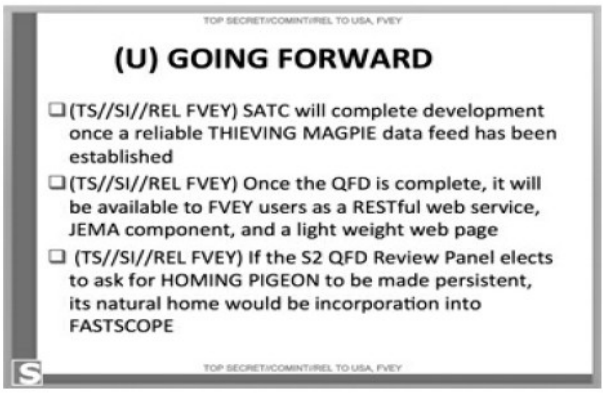
Tại hội nghị năm 2012 của 5 cặp mắt, GCHQ đã trình chiếu một chương trình can thiệp có tên là Thieving Magpie, nhằm vào sự sử dụng ngày một sẵn các điện thoại cầm tay trong các chuyến bay:

Giải pháp được đề xuất đã mường tượng một hệ thống để đảm bảo "bao trùm toàn bộ thế giới":

Sự tiến bộ đáng kể đã được thực hiện để đảm bảo rằng các thiết bị nhất định dễ bị giám sát trong các máy bay phản lực chở khách:

Một tài liệu có liên quan của NSA được trình chiếu trong cùng hội nghị đó, cho một chương trình có tên là Homing Pigeon, cũng mô tả các nỗ lực để theo dõi các giao tiếp truyền thông trong chuyến bay. Chương trình của cơ quan đó từng được phối hợp với GCHQ, và toàn bộ hệ thống được làm cho sẵn sàng cho nhóm 5 cặp mắt.

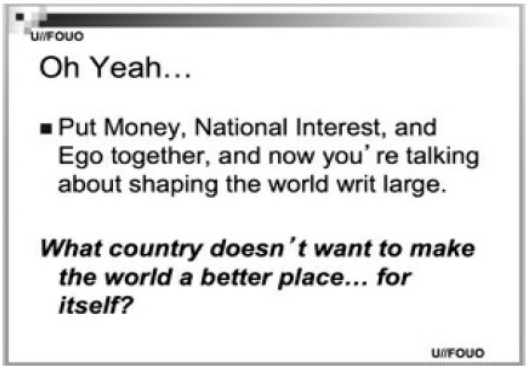




***

Có sự vô tư đáng lưu ý, trong các phần của NSA, về mục đích thực của việc xây dựng một hệ thống giám sát bí mật quá khổng lồ. Một trình chiếu PowerPoint được chuẩn bị cho một nhóm các quan chức cơ quan này thảo luận về triển vọng của các tiêu chuẩn Internet quốc tế đưa ra quan điểm không tô son điểm phấn gì. Tác giả của trình chiếu là một "Sĩ quan Tình báo Quốc gia của NSA/SIGINT (SINIO) về Khoa học và Công nghệ", tự được mô tả như là "một nhà khoa học và cao thủ được huấn luyện tốt".

Tiêu đề chân phương của bài trình bày của anh ta: "Vai trò của các lợi ích quốc gia, tiền, và cái Tôi". 3 yếu tố đó cùng nhau, anh ta nói, là động lực trước hết dẫn dắt nước Mỹ duy trì sự áp đảo giám sát toàn cầu.



Anh ta lưu ý rằng sự áp đảo của Mỹ đối với Internet đã trao cho nước này sức mạnh và tầm ảnh hưởng đáng kể, và cũng đã sinh ra lợi nhuận khổng lồ:

Lợi nhuận và sức mạnh như vậy cũng không tránh khỏi đã tích lũy, tất nhiên, cho bản thân nền công nghiệp giám sát, cung cấp động lực khác cho sự mở rộng bất tận của nó. Kỷ nguyên sau ngày 11/09 đã chứng kiến một sự bùng nổ ồ ạt các tài nguyên được dành cho sự giám sát. Hầu hết các tài nguyên đó từng được truyền từ két tiền của công chúng (nghĩa là, những người Mỹ đóng thuế) vào các túi của các tập đoàn quốc phòng giám sát tư nhân.

Các công ty như Booz Allen Hamilton và AT&T sử dụng đám người là các cựu quan chức hàng đầu của chính phủ, trong khi đám người là các quan chức quốc phòng hàng đầu hiện hành là các nhân viên trong quá khứ (và có khả năng trong tương lai) của chính các tập đoàn đó. Sự phát triển không ngừng nhà nước giám sát là một cách để đảm bảo rằng các quỹ của chính phủ giữ luôn chảy, rằng cánh cửa xoay vẫn giữ được bôi trơn. Đó cũng là cách tốt nhất để đảm bảo rằng NSA và các cơ quan có liên quan của nó vẫn giữ tầm quan trọng về mặt tổ chức và có ảnh hưởng ở Washington.

Vì phạm vi và tham vọng của nền công nghiệp giám sát gia tăng, do đó có hồ sơ đối thủ cảm thấy được của nó. Việc liệt kê các mối đe dọa khác nhau được cho là nước Mỹ đang đối mặt, NSA - trong một tài liệu có tên là "Cơ quan An ninh Quốc gia: Tóm tắt tổng quan" - đưa vào một vài khái niệm dự đoán: "các tin tặc", "các yếu tố phạm tội", và "những tên khủng bố". Tiết lộ, dù vậy, nó cũng đi rộng lớn hơn nhiều bằng việc đưa vào trong số các mối đe dọa mà một danh sách các công nghệ, bao gồm bản thân Internet:

Internet từ lâu đã được báo trước như một công cụ chưa từng thấy của sự dân chủ hóa và tự do hóa, thậm chí là sự giải phóng. Nhưng trong con mắt của chính phủ Mỹ, mạng toàn cầu này và các dạng công nghệ giao tiếp truyền thông khác đe dọa làm xói mòn sức mạnh của Mỹ. Nhìn từ quan điểm này, tham vọng của NSA để "thu thập tất cả" cuối cùng trở thành mạch lạc. Là sống còn rằng NSA theo dõi tất cả các phần của Internet và bất kỳ phương tiện giao tiếp nào khác, sao cho không gì có thể thoát ra khỏi sự kiểm soát của chính phủ Mỹ.

Kết cục, vượt ra ngoài sự điều khiển ngoại giao và thành tích kinh tế, một hệ thống gián điệp ở khắp mọi nơi cho phép nước Mỹ duy trì sự kìm kẹp của nó đối với thế giới. Khi nước Mỹ có khả năng biết được mọi điều mà mọi người đang làm, đang nói, đang nghĩ, và đang lên kế hoạch - thì các công dân của riêng nó, dân chúng nước ngoài, các tập đoàn quốc tế, các nhà lãnh đạo chính phủ khác - sức mạnh của nó đối với các phần đó được tối đa hóa. Điều đó đúng gấp đôi nếu chính phủ vận hành ở các mức bí mật lớn hơn chưa từng thấy. Sự bí mật tạo ra một tấm gương một chiều: chính phủ Mỹ thấy những gì mọi người khác trên thế giới này làm, bao gồm cả dân chúng của riêng mình, trong khi không ai thấy các hành động của riêng mình cả. Đây thực sự là sự mất cân bằng, cho phép sự nguy hiểm nhất đối với tất cả các điều kiện của con người: sự thực thi quyền lực vô hạn mà không có sự minh bạch và trách nhiệm giải trình.

Những tiết lộ của Edward Snowden đã đánh đổ động lực nguy hiểm đó bằng việc rọi ánh sáng vào hệ thống đó và cách mà nó vận hành. Lần đầu tiên, mọi người ở khắp nơi đã có khả năng học được đúng mức độ của các khả năng giám sát được tích cóp chống lại họ. Tin tức đó đã gây ra một cuộc tranh luận cường độ lớn, được duy trì liên tục trên toàn cầu một cách chính xác vì sự giám sát đó đặt ra một mối đe dọa chết người như vậy cho sự điều hành dân chủ. Nó cũng gây ra những đề xuất cải cách, một cuộc thảo luận toàn cầu về tầm quan trọng của tự do Internet và tính riêng tư trong kỷ nguyên điện tử, và một sự tính toán với câu hỏi sống còn: sự giám sát không giới hạn có nghĩa gì đối với chúng ta như những cá nhân, trong cuộc sống của riêng chúng ta?

Chương 4. Tác hại của sự giám sát

Các chính phủ trên khắp thế giới đã có những cố gắng mãnh liệt để huấn luyện cho các công dân khinh thị tính riêng tư của riêng họ. Một kinh cầu nguyện tính tầm thường quen thuộc bây giờ đã thuyết phục mọi người chịu đựng các xâm phạm nghiêm trọng trong địa hạt riêng tư của họ; thành công là những lý lẽ bào chữa mà nhiều người hoan hô khi các nhà chức trách thu thập lượng khổng lồ các dữ liệu về những gì họ nói, đọc, mua, và làm với họ.

Các nhà chức trách nhà nước đó đã được ủng hộ trong cuộc tấn công của họ vào tính riêng tư bằng một dàn đồng ca của những người có thế lực của Internet - các đối tác dường như không thể thiếu của chính phủ trong giám sát. Khi CEO Eric Schmidt của Google từng được hỏi trong một cuộc phỏng vấn của CNBC vào năm 2009 về những quan tâm đối với việc giữ lại các dữ liệu người sử dụng của công ty ông, ông đã trả lời: "Nếu bạn có thứ gì đó mà bạn không muốn bất kỳ ai biết, thì có thể bạn sẽ không nên làm điều đó ngay từ đầu". Với sự tùy tiện ngang bằng, người sáng lập và CEO của Facebook Mark Zuckerberg đã nói trong một cuộc phỏng vấn năm 2010 rằng "mọi người thực sự có sự thuận tiện không chỉ bằng việc chia sẻ thông tin và các dạng khác nhiều hơn, mà còn mở hơn và với nhiều người hơn". Tình riêng tư trong kỷ nguyên số không còn là một "chuẩn mức xã hội", ông nói, một khái niệm thuận tiện phục vụ cho những lợi ích của một công ty công nghệ đang buôn bán thông tin cá nhân.

Nhưng tầm quan trọng của tính riêng tư là bằng chứng trong thực tế rằng thậm chí những người làm cho nó mất giá, những người đã tuyến bố nó đã chết hoặc không cần thiết, cũng không tin vào những điều họ nói. Những người bảo vệ việc chống lại tính riêng tư thường đi rất xa để duy trì sự kiểm soát đối với tính có thể trông thấy được đối với hành vi và thông tin của riêng họ. Bản thân chính phủ Mỹ đã sử dụng các biện pháp cực kỳ để che chắn cho các hành động của họ khỏi bị công chúng nhìn thấy, dựng lên một bức tường bí mật cao hơn bao giờ hết mà họ đang vận hành đằng sau nó. Như một báo cáo năm 2011 từ ACLU đã viện lý, "Ngày nay nhiều nghiệp vụ của chính phủ chúng ta được tiến hành trong bí mật". Thế giới bóng tối này là quá bí mật, "quá lớn, quá khó cấm", như tờ *Washington Post* đã nêu, rằng không ai biết nó có giá bao nhiêu tiền, có bao nhiêu người nó thuê làm, có bao nhiêu chương trình đang tồn tại bên trong nó hoặc chính xác có bao nhiêu cơ quan làm công việc y hệt đó.

Tương tự, các ông trùm tư bản Internet đó hình như đang quá bằng lòng làm mất giá trị tính riêng tư của chúng ta lại đang bảo vệ mãnh liệt tính riêng tư của riêng họ. Google đã khăng khăng về một chính sách không nói cho các nhà báo từ CNET, site tin tức công nghệ, sau khi CNET đã xuất bản các chi tiết cá nhân của Eric Schmidt - bao gồm lương, các khoản quyên góp trong các chiến dịch từ thiện, và địa chỉ của ông ta, tất cả các thông tin công khai có được qua Google - để nhấn mạnh những mối nguy hiểm khổng lồ của công ty của ông.

Trong khi đó, Mark Zuckerberg đã mua 4 ngôi nhà liền kề cho riêng mình ở Palo Alto, với giá 30 triệu USD, để đảm bảo cho tính riêng tư của ông ta. Như CNET đã nêu, "cuộc sống cá nhân của bạn bây giờ được biết như là các dữ liệu của Facebook. Cuộc sống cá nhân của CEO của hãng bây giờ

được biết như doanh nghiệp của riêng trí tuệ của bạn".

Mâu thuẫn y hệt được nhiều công dân bình thường thể hiện, những người bỏ qua giá trị của tính riêng tư dù vẫn có các mật khẩu trong các tài khoản phương tiện xã hội và thư điện tử của họ. Họ để chìa khóa ở các cửa buồng tắm của họ; họ đóng triện các phong bì chứa các bức thư của họ. Họ hành xử như thể không ai đang theo dõi những gì họ có thể không bao giờ cân nhắc khi hành động công khai. Họ nói những điều cho bạn bè, các nhà tâm lý học, và các luật sư rằng họ không muốn bất cứ ai khác biết. Họ lên tiếng về các suy nghĩ trên trực tuyến rằng họ không muốn có liên quan tới các cái tên của họ.

Nhiều người bảo vệ ủng hộ giám sát mà tôi đã tranh luận kể từ khi Snowden đã thổi còi đã nhanh chóng phụ họa cho quan điểm của Eric Schmidt rằng tính riêng tư là dành cho những người mà có gì đó để dấu. Nhưng không ai trong số họ muốn trao cho tôi các mật khẩu các tài khoản thư điện tử của họ, hoặc cho phép quay video trong các ngôi nhà của họ.

Khi chủ tịch Ủy ban Tình báo Thượng viện, Dianne Feinstein, đã khăng khăng rằng sự thu thập siêu dữ liệu của NSA không tạo thành sự giám sát - vì nó không bao gồm nội dung của bất kỳ giao tiếp truyền thông nào - những người phản đối trên trực tuyến đã yêu cầu rằng bà sao lưu sự khẳng định của bà bằng hành động: Liệu thượng nghị sỹ, mỗi tháng, có xuất bản một danh sách đầy đủ những người mà bà đã gửi thư điện tử và gọi điện thoại hay không, bao gồm cả độ dài thời gian họ đã nói chuyện và các vị trí vật lý của họ khi cuộc gọi từng được thực hiện hay không? Điều mà có lẽ bà cho là không thể tưởng tượng được chính xác vì thông tin đó đang tiết lộ một cách sâu sắc; để điều đó thành công khai có thể tạo nên một lỗ hổng thực sự trong lãnh địa riêng tư của một người.

Điểm mấu chốt là không phải sự đạo đức giả của những người mà đang làm mất uy tín giá trị của tính riêng tư trong khi lại đang bảo vệ mãnh liệt cho riêng họ, dù điều đó là nổi bật. Đó là mong muốn về tính riêng tư được tất cả chúng ta chia sẻ như một phần cơ bản, không lệ thuộc của những gì có nghĩa là con người. Tất cả chúng ta theo bản năng hiểu rằng lãnh địa riêng tư là nơi chúng ta có thể hành động, suy nghĩ, nói, viết, thử nghiệm, và chọn cách để làm, nằm ngoài những con mắt soi xét của những người khác. Tính riêng tư là điều kiện cơ bản của việc là một con người tự do.

Có thể công thức nổi tiếng nhất của những gì tính riêng tư có nghĩa và vì sao nó lại quá vạn năng và tột cùng được mong mỏi đã được Louis Brandeis của Tòa án Công lý Tối cao (Supreme Court Justice) Mỹ đưa ra trong vụ kiện Olmstead ở Mỹ năm 1928: "Quyền để được ở lại một mình [là] toàn diện nhất trong các quyền, và là quyền có giá trị nhất của một con người tự do". Giá trị của tính riêng tư, ông đã viết, "là rộng lớn hơn nhiều về phạm vi" so với chỉ là các quyền tự do dân sự. Đó là, ông nói, cơ bản:

> Những người làm ra Hiến pháp đã hiểu để đảm bảo các điều kiện có lợi để mưu cầu hạnh phúc. Họ đã nhận thức được tầm quan trọng bản chất tự nhiên về tinh thần của một con người, về cảm giác và khả năng hiểu biết của con người. Họ biết rằng chỉ một phần của sự đau đớn, niềm vui và những thỏa mãn của cuộc sống sẽ được thấy trong vật chất. Họ đã tìm cách để bảo vệ những người Mỹ theo lòng tin của họ, suy nghĩ của họ, cảm xúc của họ và cảm giác của họ. Họ đã ban, như chống lại Chính phủ, quyền để được ở lại một mình.

Thậm chí trước khi Brandeis từng được bổ nhiệm tới Tòa án này, ông từng là một người đề xuất đầy nhiệt huyết về tầm quan trọng của tính riêng tư. Cùng với luật sư Samuel Warren, ông đã viết bài báo có tính hạt giống cho *Harvard Law Review* vào năm 1890 có tựa đề "*Quyền về Tính riêng tư*", viện lý rằng việc cướp đi của ai đó tính riêng tư của họ là một tội ác về bản chất tự nhiên khác xa so với hành vi trộm cắp một vật chất thuộc về [người đó]. "Nguyên tắc bảo vệ các tác phẩm cá nhân và tất cả các sản phẩm cá nhân khác, không chống lại hành vi trộm cắp và chiếm đoạt vật lý, mà chống lại sự xuất bản ở bất kỳ dạng nào, trong thực tế không phải là nguyên tắc của sở hữu tư nhân, mà là của một cá nhân bất khả xâm phạm".

Tính riêng tư là cơ bản đối với sự tự do và hạnh phúc của con người vì những lý do hiếm khi được thảo luận nhưng được hiểu theo bản năng của hầu hết mọi người, như được chứng tỏ bởi bề dài theo đó họ đi bảo vệ của riêng họ. Để bắt đầu, mọi người thay đổi triệt để hành vi của họ khi họ biết họ đang bị theo dõi. Họ sẽ phấn đấu làm điều mà họ kỳ vọng. Họ muốn tránh sự hổ thẹn và sự qui tội. Họ làm thế bằng việc gắn chặt vào các thực tiễn xã hội được chấp nhận, bằng việc ở lại bên trong các đường biên được đặt ra, tránh hành động có thể được xem là lầm đường lạc lối hoặc dị thường.

Dải những lựa chọn mà con người cân nhắc khi họ tin tưởng rằng những người khác đang theo dõi vì thế có giới hạn hơn nhiều so với những gì họ có thể làm khi hành động trong một lãnh địa riêng tư. Sự từ chối tính riêng tư vận hành bí mật sẽ hạn chế quyền tự do lựa chọn của một người.

Vài năm trước, tôi đã dự lễ bat mitzvah (lễ đánh dấu người con gái tròn 20 tuổi theo do thái giáo) con gái người bạn tốt nhất của tôi. Trong buổi lễ, giáo sĩ đã nhấn mạnh rằng "bài học trung tâm" con gái phải học là con gái "luôn đang bị theo dõi và phán xử". Ông đã nói cho cô gái rằng Chúa Trời luôn biết những gì cô gái từng làm, mọi sự lựa chọn, mọi hành động, và thậm chí mọi suy nghĩ, bất kể riêng tư thế nào. "Con sẽ không bao giờ một mình cả", ông nói, điều có nghĩa rằng cô gái sẽ luốn gắn với ý chí của Chúa Trời.

Điểm mấu chốt của giáo sĩ từng rất rõ: nếu bạn có thể không bao giờ tránh được các con mắt theo dõi của một đấng tối cao, thì sẽ không có sự lựa chọn nào ngoài phải tuân theo các mệnh lệnh mà đáng tối cao đó áp đặt. Bạn thậm chí không thể cân nhắc giả mạo theo cách riêng của bạn để vượt qua những quy tắc đó: nếu bạn tin tưởng bạn luôn bị theo dõi và phán xét, thì bạn thực sự không phải là một cá nhân tự do.

Tất cả các nhà chức trách đàn áp - chính trị, tôn giáo, xã hội, cha mẹ - dựa vào sự thực sống còn này, sử dụng nó như một công cụ nguyên tắc để thực thi tính chính thống, bắt buộc tuân thủ, và dẹp yên bất đồng chính kiến. Điều đó là theo lợi ích của họ để truyền đạt rằng không có gì các đối tượng của họ làm sẽ thoái khỏi được sự nhận biết của các nhà chức trách. Hiệu quả hơn nhiều so với một lực lượng cảnh sát, sự tước đoạt tính riêng tư sẽ nghiền nát bất kỳ sự cám dỗ nào làm trệch khỏi các qui tắc và chuẩn mực.

Những gì bị mất khi lãnh địa riêng tư bị thủ tiêu là nhiều thuộc tính điển hình có liên quan tới chất lượng của cuộc sống. Hầu hết mọi người đã trải nghiệm cách mà tính riêng tư xúc tác cho sự giải phóng khỏi ràng buộc. Và tất cả chúng ta, ngược lại, đều đã có kinh nghiệm về việc tham gia vào hành vi riêng tư khi chúng ta nghĩ chúng ta từng một mình - việc khiêu vũ, thú tội, khai thác thể

hiện tình dục, chia sẻ các ý tưởng chưa được thử nghiệm - chỉ cảm thấy xấu hổ khi bị những người khác nhìn thấy.

Chỉ khi chúng ta tin tưởng rằng không ai khác đang theo dõi chúng ta thì chúng ta mới cảm thấy tự do - an toàn - thực sự trải nghiệm, để kiểm thử các giới hạn, để khai thác các cách thức suy nghĩ mới, để khai thác những gì nó có nghĩa sẽ là của bản thân chúng ta. Những gì đã làm cho Internet thật quyến rũ từng chính xác là quá đỗi sống còn đối với sự khai thác cá nhân.

Vì lý do đó, chính trong lãnh địa riêng tư nơi mà tính sáng tạo, sự bất đồng chính kiến, và những thách thức đối với tính chính thống nảy mầm. Một xã hội trong đó mỗi người đều biết họ có thể bị nhà nước theo dõi - nơi mà lãnh địa riêng tư bị loại bỏ một cách có hiệu quả - là một xã hội trong đó các thuộc tính đó bị mất, cả ở mức xã hội và cá nhân.

Giám sát ồ ạt từ nhà nước vì thế vốn dĩ là đàn áp, thậm chí trong trường hợp không chắc có thực rằng nó không bị các quan chức hay thù oán lạm dụng để làm những điều giống như giành được thông tin riêng tư về các đối thủ chính trị. Bất kể sự giám sát được sử dụng hoặc lạm dụng như thế nào, thì những hạn chế mà nó đặt ra lên sự tự do là có thực bên trong sự tồn tại của nó.

***

Việc viện tới George Orwell năm 1984 là thứ gì đó sáo rỗng, nhưng những phụ họa của thế giới về những gì ông ta đã cảnh báo trong sự giám sát nhà nước của NSA là không sai: cả 2 đều dựa vào sự tồn tại của một hệ thống công nghệ với khả năng giám sát các hành động và ngôn luận của từng công dân. Sự tương tự bị các nhà vô địch giám sát từ chối - chúng ta không phải lúc nào cũng bị theo dõi, họ nói - nhưng lý lẽ đó là không trúng. Vào năm 1984, các công dân từng không nhất thiết bị theo dõi mọi lúc; trong thực tế, họ đã không biết liệu họ có bao giờ thực sự bị theo dõi hay không. Nhưng nhà nước đã có khả năng theo dõi họ bất cứ lúc nào. Đó từng là điều không chắc chắn và khả năng giám sát mọi lúc mọi nơi đã phục vụ để giữ cho từng người trong khuôn khổ:

> Màn hình đã nhận được và truyền đi cùng một lúc. Bất kỳ tiếng động nào mà Winston đã tạo ra, trên mức của sự thì thầm rất nhỏ, có thể bị nó ghi lại; hơn nữa, miễn là anh ta vẫn ở trong tầm nhìn mà tấm kim loại đó chỉ huy, anh ta có thể bị nhìn thấy cũng như bị nghe thấy. Tất nhiên từng không có cách gì để biết liệu bạn có đang bị theo dõi hay không ở bất kỳ lúc nào. Thường xuyên tới đâu, hoặc hệ thống nào, Cảnh sát Tư duy (Thought Police) được cài cắm ở bất kỳ đường dây cá nhân nào từng là sự phỏng đoán. Thậm chí có thể tưởng tượng được là họ đã theo dõi từng người ở mọi lúc. Nhưng ở bất kỳ mức độ nào họ cũng có thể cài cắm vào đường dây của bạn bất kỳ khi nào họ muốn. Bạn đã phải sống - đã sống, từ thói quen mà đã trở thành bản năng - trong sự thừa nhận rằng mỗi tiếng động bạn tạo ra đều đã bị nghe trộm, và ngoại trừ trong bóng tối, mỗi cử động đều bị soi xét.

Thậm chí NSA, với khả năng của nó, có thể không đọc từng thư điện tử, nghe từng cuộc gọi điện thoại, và dõi theo các hành động của từng cá nhân. Những gì làm cho một hệ thống giám sát có hiệu quả trong việc kiểm soát hành vi của con người là tri thức mà các lời nói và hành động của một người đều đáng ngờ đối với việc giám sát.

Nguyên lý này từng ở trong tâm của khái niệm về Nhà tù xây tròn (Panopticon) ở thế kỷ 18 của nhà triết học người Anh Jeremy Bentham, một thiết kế xây dựng mà ông ta đã tin tưởng có thể cho phép các cơ quan kiểm soát có hiệu quả các hành vi của con người. Cấu trúc của tòa nhà sẽ được sử dụng, theo ngôn từ của ông ta, vì "bất kỳ dạng thiết lập nào, theo đó mọi người theo bất kỳ sự mô tả nào cũng sẽ được nằm dưới sự kiểm tra". Đổi mới về kiến trúc ban đầu của Panopticon từng là một cái tháp trung tâm lớn mà từ đó từng căn phòng - hoặc ô, hoặc lớp học, hoặc khu vực - có thể được những người canh gác theo dõi bất kỳ lúc nào. Tuy nhiên, các cư dân đã không có khả năng để nhìn vào trong tòa tháp và vì thế có thể không bao giờ biết liệu họ có hay không bị theo dõi.

Vì cơ quan đó - bất kỳ cơ quan nào - từng không có khả năng quan sát thấy tất cả mọi người tất cả mọi lúc, nên giải pháp của Bentham từng là để "có vẻ như tạo ra sự có mặt của người theo dõi ở khắp mọi nơi" trong trí óc của các cư dân. "Những người bị theo dõi sẽ luôn cảm thấy bản thân họ dường như đang bị theo dõi, ít nhất là có cơ hội lớn để làm được như vậy". Họ có thể vì thế hành động như thể họ từng luôn bị theo dõi, thậm chí nếu họ không bị. Kết quả có thể là sự tuân thủ, vâng lời, và tuân theo các kỳ vọng. Bentham đã mường tượng rằng sáng tạo của ông ta có thể lan truyền vươn xa tới các nhà tù và các bệnh viện tâm thần tới tất cả các cơ quan xã hội. Việc khắc sâu vào trí nhớ của các công dân rằng họ có thể luôn bị theo dõi có khả năng, theo ông ta hiểu, cách mạng hóa hành vi của con người.

Vào những năm 1970, Michel Foucault đã quan sát thấy rằng nguyên tắc Panopticon của Bentham từng là một trong những cơ chế nền tảng của nhà nước hiện đại. Trong cuốn *Sức mạnh* (*Power*), ông đã viết rằng Panopticonism là "một dạng sức mạnh được áp dụng cho các cá nhân ở dạng của sự giám sát cá nhân liên tục, ở dạng của sự kiểm soát, trừng phạt, và đền bù, và ở dạng của sự sửa cho đúng, đó là, sự đúc kết và biến đổi các cá nhân theo các điều khoản theo các chuẩn mực nhất định".

Trong *Nguyên tắc và Trừng phát* (*Discipline and Punish*), Foucault đã giải thích xa hơn rằng giám sát ở khắp mọi nơi không chỉ trang bị cho các nhà chức trách và bắt phải tuân thủ, mà còn xui khiến các cá nhân quốc tế hóa những giám sát của họ. Những người tin tưởng họ đang bị giám sát, theo bản năng sẽ chọn làm những gì họ muốn mà thậm chí không nhận thức được rằng họ đang bị kiểm soát - Panopticon xui khiến "tù nhân ở vào trạng thái của tính có thể nhìn thấy được một cách có ý thức và thường trực mà đảm bảo vận hành sức mạnh một cách tự động". Với sự kiểm soát được quốc tế hóa, bằng chứng không úp mở về sự đàn áp sẽ biến mất vì nó không còn cần thiết nữa: "sức mạnh bên ngoài có thể ném đi sức nặng vật lý của nó; nó có xu hướng không phải là thể xác; và nó càng tiếp cận giới hạn này bao nhiêu, thì các hiệu quả của nó càng liên tục, sâu sắc và thường trực bấy nhiêu: đây là một thắng lợi sâu sắc mà tránh được bất kỳ sự phản đối vật lý nào và nó luôn được quyết định trước".

Bổ sung thêm, mô hình kiểm soát này có ưu thế lớn vì cùng một lúc tạo ra sự ảo tưởng về sự tự do. Sự cưỡng bách và sự phục tùng tồn tại trong tâm trí các cá nhân. Các cá nhân chọn cho riêng mình để tuân thủ, ngoài nỗi sợ hãi rằng họ đang bị theo dõi. Điều đó loại bỏ nhu cầu đối với tất cả các dấu xác nhận cưỡng bách có thể nhìn thấy được, và vì thế xúc tác cho sự kiểm soát đối với mọi người mà tin tưởng sai lầm vào bản thân họ là được tự do.

Vì lý do này, mọi nhà nước đàn áp xem sự giám sát như một trong những công cụ kiểm soát sống còn nhất của mình. Khi thủ tướng Angela Merkel của Đức bị ức chế đã học được rằng NSA đã bỏ ra nhiều năm nghe lén điện thoại cầm tay cá nhân của bà, thì bà đã nói cho Tổng thống Obama và cáu giận so sánh sự giám sát của Mỹ như Stasi, cơ quan dịch vụ an ninh nổi tiếng của Đông Đức, nơi mà bà đã lớn lên. Merkel đã không ngụ ý rằng nước Mỹ từng là sự tương đồng với chế độ cộng sản; thay vào đó là sự tồn tại thực tế của một nhà nước giám sát đầy hăm dọa, nó có thể là NSA hoặc Stasi hoặc ông Anh Lớn (Big Brother) hoặc Panopticon, là tri thức mà một người có thể bị các nhà chức trách tàng hình theo dõi bất cứ lúc nào.

***

Không khó để hiểu vì sao các nhà chức trách ở Mỹ và các quốc gia phương Tây khác đã từng bị cám dỗ để xây dựng một hệ thống gián điệp ở khắp mọi nơi nhằm vào các công dân của riêng họ.

Bất bình đẳng về kinh tế tồi tệ hơn, được biến thành một cuộc khủng hoảng toàn diện với sự sụp đổ tài chính trong năm 2008, đã tạo ra sự bất ổn nội bộ chết người. Đã có sự nổi dậy nhìn thấy được thậm chí ở các nền dân chủ khá ổn định, như Tây Ban Nha và Hy Lạp. Vào năm 2011, đã có những ngày nổi loạn ở Luân Đôn. Tại nước Mỹ cả cánh hữu - những người phản đối của *Tea Party* (*Đảng Chè*) trong các năm 2008 và 2009 - và cánh tả - phong trào *Chiếm đóng* (*Occupy*) - đã phát động các cuộc phản đối dài lâu của các công dân. Các cuộc thăm dò dư luận ở các nước đó đã tiết lộ các mức độ căng thẳng nổi bật của sự bất đồng chính kiến với tầng lớp chính trị và đường lối xã hội.

Các nhà chức trách đã đối mặt với sự nổi dậy thường có 2 lựa chọn: xoa dịu dân chúng bằng các nhượng bộ có tính biểu tượng hoặc củng cố sự kiểm soát của họ để giảm thiểu tác hại mà nó có thể gây ra cho những lợi ích của họ. Giới tinh hoa ở phương Tây dường như thấy sự lựa chọn thứ 2 - việc tăng cường sức mạnh của họ - như là lý do tốt hơn, có lẽ sống được duy nhất của họ để bảo vệ quan điểm của họ. Câu trả lời cho phong trào *Chiếm đóng* từng là ép nó bằng sức mạnh, thông qua xịt khí, bơm cay, và khởi tố. Các lực lượng cảnh sát bán quân sự nội địa từng hiện diện đầy trong các thành phố ở Mỹ, như các sĩ quan cảnh sát mang vũ khí được thấy trên các đường phố ở Baghdad để đàn áp những người phản đối tụ tập hợp pháp và phần lớn là trong hòa bình. Chiến lược đó đã đặt mọi người vào nỗi sợ hãi tham dự các cuộc tuần hành và phản đối, và nó thường làm được việc. Mục đích thông thường hơn từng là để phá ý nghĩa rằng dạng phản kháng này là không có hiệu quả chống lại một lực lượng được thiết lập không thể xuyên thủng và đồ sộ.

Một hệ thống giám sát ở khắp mọi nơi đạt được mục tiêu y hệt nhưng thậm chí với sức mạnh lớn hơn. Việc tổ chức các phong trào bất đồng chính kiến chỉ đơn thuần trở thành khó khăn khi chính phủ đang theo dõi mọi điều mà mọi người đang làm. Nhưng sự giám sát ồ ạt cũng giết đi sự bất đồng chính kiến ở nơi quan trọng hơn và sâu hơn: trong tâm trí, nơi mà các đoàn xe cá nhân chỉ nghĩ phù hợp với những gì được kỳ vọng và được yêu cầu.

Lịch sử để lại không nghi ngờ gì rằng sự ép buộc và kiểm soát hợp tác là tất cả ý định và hiệu lực của sự giám sát nhà nước. Nhà viết kịch bản phim Hollywood Walter Bernstein, người từng bị đưa vào danh sách đen và bị giám sát trong kỷ nguyên của McCarthy, bị ép phải viết dưới bí danh để tiếp tục làm việc, đã mô tả động cơ của sự tự kiểm duyệt ngột ngạt tới từ ý nghĩ đang bị giám sát:

> Từng người đều đã thận trọng. Đó không phải là thời điểm để mạo hiểm nói ... Đã có những nhà văn, những nhà văn không nằm trong danh sách đen mà đã nói, tôi không biết bạn có thể gọi họ là gì, "những điều tiên tiến" (cuttingedge things), nhưng không phải là chính trị. Họ tránh xa khỏi chính trị... tôi nghĩ đã có cảm giác chung về "Bạn đừng có gắn cổ của bạn ra". Đó không phải là bầu không khí giúp cho sự sáng tạo hoặc để cho trí óc được tự do. Bạn luôn ở trong nguy hiểm của sự tự kiểm duyệt, nói "không, tôi sẽ không thử điều này vì tôi biết nó sẽ không được hoàn thành hoặc nó sẽ làm xa lánh chính phủ", hoặc thứ gì đó tương tự.

Những quan sát của Bernstein từng được bắt chước một cách kỳ lạ trong một báo cáo được *PEN America* phát hành vào tháng 11/2013 với đầu đề *Các Hiệu ứng Phát ớn: Sự giám sát của NSA dẫn các nhà văn Mỹ tới sự tự kiểm duyệt* (*Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*). Tổ chức đó đã tiến hành một khảo sát xem xét các hiệu ứng của những tiết lộ của NSA lên các thành viên của nó, phát hiện ra rằng nhiều nhà văn bây giờ "giả thiết rằng các giao tiếp truyền thông của họ đang bị theo dõi" và đã thay đổi hành vi của họ theo các cách thức mà "cắt bớt đi tự do ngôn luận của họ và hạn chế dòng chảy tự do của thông tin". Đặc biệt, "24% đã có chủ ý tránh các chủ đề nhất định trong các trao đổi trên điện thoại và thư điện tử".

Sức mạnh kiểm soát tai hại của sự giám sát ở khắp mọi nơi và sự tự kiểm duyệt mà các kết quả được khẳng định trong một dải các thí điểm khoa học xã hội và mở rộng vượt xa ra khỏi hoạt động chính trị xã hội. Nhiều nghiên cứu chỉ ra động cơ này làm việc thế nào ở các mức độ tâm lý và cá nhân sâu nhất.

Một đội các nhà nghiên cứu, xuất bản các phát hiện của họ trong tạp chí *Tâm lý học Tiến hóa* (*Evolutionary Psychology*), đã trình bày các đối tượng của họ với các hành động nghi ngờ về đạo đức, như việc giữ một lượng tiền lớn được thấy trong một chiếc ví trên đường hoặc biết rằng một người bạn đã bổ sung thêm thông tin sai vào lý lịch cá nhân của anh ta. Các đối tượng từng được yêu cầu phải đánh giá mức độ sai trái. Nghiên cứu đã lưu ý rằng các đối tượng mà họ từng bị chỉ ra bằng các hình ảnh gợi ý trong sự giám sát, như một đôi mắt nhìn chằm chằm, đã xếp các hành động đó như là "đáng trách" hơn so với những người mà từng được chỉ ra bằng một hình ảnh trung tính. Các nhà nghiên cứu đã kết luận rằng sự giám sát khuyến khích những người đang bị theo dõi "khẳng định sự chứng thực của họ đối với các chuẩn mực xã hội đang thịnh hành" khi họ định "tích cực quản lý các uy tín của họ".

Một thí điểm toàn diện được tiến hành trong năm 1975 của các nhà tâm lý học của đại học Stanford là Gregory White và Philip Zimbardo với đầu đề "*Các hiệu ứng phát ớn của sự giám sát*" (*The Chilling Effects of Surveillance*), đã tìm cách đánh giá liệu việc đang bị theo dõi có ảnh hưởng tới sự thể hiện các ý kiến chính trị gây tranh cãi hay không. Động lực cho nghiên cứu này từng là những lo ngại của những người Mỹ về sự giám sát của chính phủ:

> Vụ lùm xùm Watergate, những tiết lộ của việc gài rệp Nhà Trắng, và những cuộc điều tra của Quốc hội về việc gián điệp nội bộ của Cục Tình báo Trung ương - CIA (Central Intelligence Agency) đã phục vụ để nhấn mạnh chủ đề hoang tưởng đang phát triển trong cuộc sống Mỹ: người Anh Lớn có lẽ đang theo dõi bạn! Các đề xuất cho các ngân hàng dữ liệu quốc gia, sử dụng các máy bay trực thăng giám sát của các lực lượng cảnh sát đô thị, sự hiện diện của các máy ghi hình quan sát trong các ngân hàng và siêu thị, và các cuộc tìm kiếm an ninh sân bay những cá nhân và tài sản là một số dấu hiệu rằng cuộc sống riêng tư của chúng ta đang được đặt dưới sự soi xét kỹ lưỡng như vậy.

Những người tham gia từng được đặt dưới các mức độ giám sát khác nhau và được yêu cầu đưa ra quan điểm của họ về sự hợp pháp hóa của cần sa.

Hóa ra là các đối tượng "bị đe dọa" - những người từng được nói rằng các tuyên bố của họ có thể được chia sẻ với cảnh sát "cho những mục đích huấn luyện" - có khả năng nhiều hơn để tố cáo sử dụng cần sa và để sử dụng các đại từ nhân xưng thứ 2 hoặc thứ 3 ("bạn", "họ", "mọi người") trong ngôn ngữ của họ. Chỉ 44% những đối tượng dưới sự giám sát đã bảo vệ cho sự hợp pháp hóa, so với 77% những người không bị "đe dọa" như vậy. Cũng nói, 31% những người tham gia đang bị giám sát cùng một lúc đã tìm kiếm sự phê chuẩn từ các nhà nghiên cứu (yêu cầu, ví dụ, "Điều đó là đúng chứ?"), trong khi chỉ 7% của nhóm khác đã làm thế. Những người tham gia mà từng "bị đe dọa" cũng đã ghi điểm cao hơn đáng kể về cảm giác lo âu và kiềm chế.

White và Zimbardo đã lưu ý trong kết luận của họ rằng "mối đe dọa hoặc thực tế giám sát của chính phủ có thể cấm tự do ngôn luận về mặt tâm lý". Họ đã bổ sung thêm rằng trong khi "thiết kế nghiên cứu của họ đã không cho phép khả năng 'tránh hội đồng'", thì họ đã kỳ vọng rằng "mối lo do sự đe dọa giám sát tạo ra có thể làm cho nhiều người hoàn toàn tránh các tình huống" trong đó họ có thể bị giám sát. "Vì những giả thiết như vậy là có giới hạn chỉ bằng sự tưởng tượng của bạn và hàng ngày được khuyến khích bởi những tiết lộ về sự xâm lấn tính riêng tư của chính phủ và các cơ quan", họ đã viết, nên "các đường biên giới giữa những ảo tưởng hoang tưởng và các lý do được minh chứng quả thực đã trở nên nhỏ, tế nhị".

Đúng là sự giám sát có thể nhiều khi thúc đẩy những gì một số người có thể xem như là hành vi mong muốn. Một nghiên cứu đã thấy rằng hành vi phá rối trật tự ở các sân vận động bóng đá ở Thụy Điển - những người hâm mộ ném các chai lọ và pháo sáng vào sân - đã giảm tới 65% sau khi giới thiệu các máy quay an ninh. Và các tài liệu y tế cộng đồng về việc rửa tay lặp đi lặp lại đã khẳng định rằng cách để làm gia tăng khả năng của ai đó rửa tay của anh hoặc chị ta là đặt ai đó ở gần đó.

Nhưng một cách áp đảo, hiệu ứng đang bị theo dõi là đối với sự lựa chọn cưỡng ép cá nhân nghiêm trọng. Thậm chí trong các thiết lập thân mật nhất, trong gia đình, ví dụ, thì sự giám sát sẽ biến các hành động không quan trọng thành một nguồn tự phán xét và lo lắng, chỉ vì thực tế đang bị quan sát. Trong một thí điểm ở nước Anh, các nhà nghiên cứu đã đưa ra các đối tượng với các thiết bị

theo dõi để giữ các nhãn (tab) trong các thành viên gia đình. Vị trí chính xác của bất kỳ thành viên nào cũng truy cập được bất kỳ lúc nào, và nếu vị trí của ai đó đã bị phát hiện ra, thì anh ta có thể nhận được một thông điệp. Mỗi lần một thành viên đã dõi theo một thành viên khác, anh ta cũng từng được gửi một bảng câu hỏi, hỏi vì sao anh ta đã làm thế và liệu thông tin nhận được có khớp với các kỳ vọng hay không.

Trong bản tóm tắt, những người tham gia đã nói rằng trong khi họ đôi lúc thấy việc theo dõi là thuận tiện, thì họ cũng cảm thấy lo rằng nếu họ bị ở trong một nơi không như mong đợi, thì các thành viên gia đình có thể "nhảy tới các kết luận" về hành vi của họ. Và lựa chọn về "đi mất dạng" - việc khóa cơ chế chia sẻ vị trí - đã không giải quyết được sự lo lắng đó: nhiều thành viên nói rằng hành động tránh giám sát đến đối với bản thân có thể tạo ra sự nghi ngờ. Các nhà nghiên cứu đã kết luận:

> Có các dấu vết trong cuộc sống hàng ngày của chúng ta mà chúng ta không thể giải thích mà có thể hoàn toàn là quan trọng. Tuy nhiên, sự trình diễn của chúng qua một thiết bị lần vết... trao cho chúng tầm quan trọng, dường như kêu gọi một mức trách nhiệm giải trình lớn khác thường. Điều này tạo ra các mối lo, đặc biệt trong các mối quan hệ gần gũi, trong đó mọi người có thể cảm thấy dưới sức ép lớn hơn phải tính tới những điều mà họ đơn giản không thể tính tới.

Đối với một thí điểm của Phần Lan mà đã triển khai một trong những mô phỏng giám sát triệt để nhất, các máy quay đã được đặt trong các ngôi nhà của các đối tượng - các buồng tắm và các buồng ngủ được loại trừ - và tất cả các giao tiếp truyền thông điện tử của họ đã bị theo dõi. Dù quảng cáo cho nghiên cứu đó đã lan rộng trên các phương tiện xã hội, các nhà nghiên cứu đã gặp khó khăn thậm chí để có 10 hộ gia đình tham gia.

Trong số những người đã đăng ký, những than phiền về dự án đã tập trung vào sự xâm lấn các phần thông thường trong cuộc sống hàng ngày của họ. Một người đã cảm thấy không tiện khi đang trần truồng trong ngôi nhà của cô ta; người khác đã cảm thấy có ý thức về các máy quay trong khi sửa tóc của cô ta trước một vòi tắm; một số khác đã nghĩ về sự giám sát trong khi tiêm thuốc y tế. Các hành động vô thưởng vô phạt đã giành được các lớp quan trọng khi bị giám sát.

Các đối tượng ban đầu đã mô tả sự giám sát như là gây phiền nhiễu; tuy nhiên, họ sớm "quen với nó". Những gì đã bắt đầu như là xâm lấn sâu sắc đã trở thành được bình thường hóa, được biến đổi thành tình trạng công việc thông thường và không còn được lưu ý nữa.

Như các thí điểm đã chỉ ra, có tất cả các dạng những điều mà mọi người làm mà họ hăng hái để giữ tính riêng tư, thậm chí dù các dạng điều đó không tạo thành việc làm "thứ gì đó sai". Tính riêng tư là không thể thiếu được đối với một dải rộng lớn các hoạt động của con người. Nếu ai đó gọi một đường dây tự tử hoặc thăm một nhà cung cấp nạo phá thai hoặc hay lui tới một website tình dục trực tuyến hoặc thực hiện một cuộc hẹn với một phòng khám phục hồi chức năng hoặc chữa bệnh, hoặc nếu một người thổi còi gọi một nhà báo, thì có nhiều lý do cho việc giữ các hành động như vậy là riêng tư mà không có mối liên hệ nào tới tính bất hợp pháp hay làm sai cả.

Tóm lại, mỗi người có thứ gì đó để ẩn dấu. Nhà báo Barton Gellman đã nêu điểm đó theo cách này:

> Tính riêng tư là có quan hệ. Nó phụ thuộc vào khán phòng của bạn. Bạn không muốn ông chủ của bạn biết bạn đang săn lùng công việc. Bạn không tuôn ra tất cả cuộc sống tình yêu của bạn cho mẹ bạn, hoặc cho những đứa con của bạn. Bạn không nói các bí mật thương mại của bạn cho các đối thủ cạnh tranh của bạn. Chúng ta không tiết lộ bản thân chúng ta một cách bừa bãi và chúng ta quan tâm đủ về bóc trần nói dối như một vấn đề về tiến trình. Trong các công dân thẳng thắn, các nhà nghiên cứu luôn thấy rằng việc nói dối là "một sự tương tác xã hội thường ngày" (2 lần trong ngày giữa các sinh viên đại học, một lần trong ngày trong Thế giới Thực)... Sự minh bạch toàn diện là một cơn ác mộng ... Mỗi người có thứ gì đó để ẩn dấu.

Lý lẽ bào chữa ban đầu cho sự giám sát - rằng đó là vì lợi ích của dân chúng - dựa vào việc bảo vệ quan điểm của thế giới mà chia các công dân thành các chủng loại người tốt và người xấu. Theo cách đó, các nhà chức trách sử dụng sức mạnh giám sát của họ chỉ để chống lại những người xấu, những người đang "làm gì đó sai", và chỉ họ có những điều để sợ sự xâm lấn tính riêng tư. Đây là một chiến thuật cũ. Trong một bài báo của tạp chí *Time* năm 1969 về những lo ngại gia tăng của người Mỹ về sức mạnh giám sát của chính phủ Mỹ, tổng chưởng lý của Nixon, John Mitchell, đã đảm bảo với các độc giả rằng "bất kỳ công dân nào của nước Mỹ mà không có liên quan trong một số hoạt động bất hợp pháp thì không có gì phải lo lắng cả".

Điểm này đã được nhắc một lần nữa từ người phát ngôn của Nhà Trắng, khi trả lời cho tranh luận năm 2005 về chương trình nghe lén bất hợp pháp của Bush: "Điều này không phải là về việc giám sát các cuộc gọi điện thoại được thiết kế để dàn xếp thực tiễn của *Little League* (*Liên đoàn Nhỏ*) hoặc mang cái gì tới một bữa ăn mỗi người góp một thứ. Chúng được thiết kế để giám sát các cuộc gọi từ những người rất xấu tới những người rất xấu". Và khi Tổng thống Obama đã xuất hiện trên chương trình *The Tonight Show* (*Chương trình tối nay*) vào tháng 08/2013 và từng được Jay Leno hỏi về những tiết lộ về NSA, ông đã nói: "Chúng ta không có một chương trình gián điệp nội địa. Những gì chúng ta có là một vài cơ chế mà có thể theo dõi một số điện thoại hoặc một địa chỉ thư điện tử được kết nối tới một cuộc tấn công khủng bố".

Đối với nhiều người, lý lẽ này làm việc. Nhận thức rằng giám sát ồ ạt chỉ được khẳng định đối với một nhóm thiệt thòi và xứng đáng của những người "đang làm sai" - những người xấu - đảm bảo rằng đa số ưng thuận với sự lạm dụng sức mạnh hoặc thậm chí khoái trá với nó.

Nhưng quan điểm đó hiểu sai một cách triệt để những mục tiêu nào dẫn dắt tất cả các cơ quan có quyền lực. "Làm thứ gì đó sai trái", trong con mắt của các cơ quan như vậy, nhấn mạnh nhiều hơn nhiều so với các hành động bất hợp pháp, hành vi vi phạm, và các âm mưu của những kẻ khủng bố. Nó điển hình mở rộng bất đồng chính kiến có ý nghĩa và bất kỳ thách thức có thực nào. Đây là bản chất tự nhiên của quyền lực để san bằng với những điều làm sai, hoặc ít nhất với một mối đe dọa.

Hồ sơ đó ngập tràn với các ví dụ về các nhóm và cá nhân đang đặt dưới sự giám sát của chính phủ bằng đức hạnh của những quan điểm và hoạt động xã hội bất đồng chính kiến của họ - Martin

Luther King, phong trào các quyền dân sự, những người hoạt động xã hội chống chiến tranh, các nhà bảo vệ môi trường. Trong con mắt của chính phủ và FBI của Edgar Hoover, tất cả họ từng là "đã làm gì đó sai": hoạt động chính trị mà đã đe dọa trật tự đang thịnh hành.

Không ai hiểu tốt hơn là Hoover sức mạnh của giám sát để vò nát sự bất đồng chính kiến về chính trị, đối đầu như ông ta đã từng với thách thức làm thế nào để ngăn chặn sự thực thi các quyền của Sửa đổi bổ sung thứ Nhất về ngôn luận và đoàn thể khi tình trạng đó bị cấm đối với việc bắt người vì việc thể hiện quan điểm không phổ biến. Được mở ra trong những năm 1960 trong một loạt các vụ kiện ở Tòa án Tối cao mà đã thiết lập các bảo vệ mạnh mẽ cho tự do ngôn luận, lên tới cực điểm trong quyết định nhất trí năm 1969 ở Brandenburg v. Ohio, nó đã lật đổ án hình sự của một lãnh đạo Ku Klux Klan (3K), người đã de dọa vi phạm chống lại các quan chức chính trị trong một bài nói chuyện. Tòa án đã nói rằng Sửa đổi bổ sung thứ Nhất đảm bảo tự do ngôn luận và tự do báo chí là mạnh tới mức mà họ "không cho phép một Nhà nước cấm hoặc đặt ra ngoài vòng pháp luật sự bảo vệ của sử dụng sức mạnh".

Đưa ra những đảm bảo đó, Hoover đã thiết lập nên một hệ thống để ngăn chặn bất đồng chính kiến từ việc phát triển nó ngay từ đầu.

Chương trình phản gián nội địa của FBI, COINTELPRO, lần đầu từng được tiết lộ từ một nhóm các nhà hoạt động xã hội chống chiến tranh mà họ đã trở nên bị thuyết phục rằng phong trào chống chiến tranh từng bị thâm nhập, bị đặt dưới sự giám sát, và bị ngắm đích bằng tất cả các dạng mưu mẹo bẩn thỉu. Thiếu bằng chứng tài liệu để chứng minh nó và không thành công trong việc thuyết phục các nhà báo để viết về những mối nghi ngờ của họ, họ đã đột nhập vào văn phòng chi nhánh FBI ở Pennsylvania vào năm 1971 và đã chở đi hàng ngàn tài liệu.

Các hồ sơ có liên quan tới COINTELPRO đã chỉ ra FBI đã nhằm vào các nhóm chính trị và các cá nhân mà nó cho là có tính lật đổ và nguy hiểm như thế nào, bao gồm cả *Liên đoàn Quốc gia về sự Tiến bộ của Người da màu*, các phong trào của những người dân tộc chủ nghĩa da đen, các tổ chức xã hội chủ nghĩa và cộng sản chủ nghĩa, những người phản đối chống chiến tranh, và các nhóm cánh hữu khác. Phòng đó đã thanh lọc họ với các đặc vụ mà họ, trong số những điều khác, đã cố gắng để điều khiển các thành viên để đồng ý thực hiện hành vi phạm tội để FBI có thể bắt giữ và truy tố họ.

FBI đã thành công trong việc thuyết phục tờ *New York Times* giữ lại các tài liệu và thậm chí trả cho họ, nhưng tờ *Washington Post* đã xuất bản một loạt các bài báo dựa vào chúng. Những tiết lộ đó đã dẫn tới sự tạo ra *Ủy ban Giáo hội Thượng viện* (*Senate Church Committee*), nó đã kết luận:

> [Trong quá trình 15 năm] Văn phòng đó đã tiến hành hoạt động ép tuân thủ luật tinh vi phức tạp thực tình nhằm vào việc ngăn chặn sự thực thi các quyền ngôn luận và hội đoàn theo Sửa đổi bổ sung thứ Nhất, về lý thuyết điều đó ngăn chặn sự phát triển của các nhóm nguy hiểm và sự tuyên truyền các ý tưởng nguy hiểm có thể bảo vệ an ninh quốc gia và ngăn chặn bạo lực.
>
> Nhiều kỹ thuật được sử dụng có thể không chịu đựng nổi trong một xã hội dân chủ thậm chí nếu tất cả các mục tiêu từng có liên quan trong hoạt động vi phạm, nhưng COINTELPRO

> đã đi vượt xa ra khỏi điều đó. Tiên đề chính không được kỳ vọng của các chương trình đó từng là một cơ quan ép tuân thủ luật có trách nhiệm tiến hành bất kỳ điều gì là cần thiết để đấu tranh với các mối đe dọa được thừa nhận đối với trật tự xã hội và chính trị đang tồn tại.

Một bản ghi chép chính của COINTELPRO đã giải thích rằng "chứng hoang tưởng" có thể được gieo trong các nhà hoạt động xã hội chống chiến tranh bằng việc để họ tin là có "một đặc vụ của FBI đứng đằng sau từng hộp thư". Theo cách này, những người bất đồng chính kiến, luôn được thuyết phục rằng họ từng bị giám sát, có thể sẽ bị dìm chết trong nỗi sợ hãi và tránh xa các hoạt động xã hội.

Không ngạc nhiên, chiến thuật đó đã làm việc. Trong một tài liệu năm 2013 có đề ngày từ năm 1971, vài trong số các nhà hoạt động xã hội đã mô tả cách mà FBI của Hoover từng "qua tất cả" phong trào các quyền dân sự với những người thâm nhập và giám sát, những người mà họ tới các cuộc họp và lớn lên.

Khi đó, thậm chí hầu hết các cơ quan bị bao vây ở Washington đã hiểu rằng chỉ đơn thuần sự tồn tại của giám sát của chính phủ, bất kể nó được sử dụng như thế nào, sẽ bóp nghẹt khả năng bất đồng chính kiến. Tờ *Washington Post*, trong một xuất bản vào tháng 03/1975 về vụ đột nhập, đã cảnh báo chính xác về động lực đàn áp này:

> FBI đã không bao giờ chỉ ra nhiều sự nhạy cảm đối với hiệu ứng độc hại mà sự giám sát của nó, và đặc biệt sự dựa dẫm của nó vào những người chỉ điểm vô danh, có khi dựa vào tiến trình dân chủ và có khi dựa vào thực tiễn của tự do ngôn luận. Nhưng đó phải là bằng chứng hiển nhiên rằng sự thảo luận và tranh cãi về các chính sách và chương trình của chính phủ bị ràng buộc sẽ bị ức chế nếu nó được biết rằng ông Anh Lớn (Big Brother), dưới sự ngụy trang, đang nghe ngóng họ và báo cáo về họ.

COINTELPRO còn xa mới là lạm dụng giám sát duy nhất được *Ủy ban Giáo hội* tìm thấy. Báo cáo cuối cùng của nó đã nêu rằng "hàng triệu bức điện tín riêng tư được gửi từ, tới, hoặc qua nước Mỹ đã bị Cơ quan An ninh Quốc gia lấy được từ 1947 tới 1975 dưới một dàn xếp bí mật với các công ty điện tín của nước Mỹ". Hơn nữa, "khoảng 300.000 cá nhân đã bị đánh chỉ số trong hệ thống máy tính của CIA và các hồ sơ riêng rẽ đã được tạo ra về khoảng 7.200 người Mỹ và hơn 100 nhóm nội địa" trong một chiến dịch của CIA, CHAOS (1967-1973).

Hơn nữa, "ước tính 100.000 người Mỹ từng là các đối tượng của các hồ sơ tình báo của Quân đội Mỹ được tạo ra giữa những năm 1960 và 1971" cũng như khoảng 11.000 cá nhân và nhóm từng bị Dịch vụ Doanh thu Nội bộ (Internal Revenue Service) điều tra "trên cơ sở chính trị hơn là các tiêu chí về thuế". Văn phòng đó cũng đã sử dụng việc nghe lén để phát hiện các chỗ bị tổn thương, như hoạt động tình dục, nó sau đó từng được triển khai để "vô hiệu hóa" các mục tiêu của họ.

Các sự việc như vậy từng không phải là những điều khác thường của kỷ nguyên đó. Trong những năm tháng của Bush, ví dụ, các tài liệu mà ACLU có được đã tiết lộ, khi nhóm này đặt nó vào năm

2006, "các chi tiết mới về giám sát của Lầu 5 góc đối với những người Mỹ chống lại cuộc chiến tranh ở Iraq, bao gồm cả các tín đồ Quaker và các nhóm sinh viên". Lầu 5 góc từng "giữ các nhãn về những người chống đối không bạo lực bằng việc thu thập thông tin và lưu trữ nó trong một cơ sở dữ liệu chống khủng bố của quân đội". ACLU đã lưu ý rằng một tài liệu, "được gắn nhãn 'hoạt động khủng bố tiềm tàng', liệt kê các sự kiện như '*Dừng Chiến tranh BÂY GIỜ*!' (*Stop the War NOW*!) tập hợp ở Akron, Ohio".

Bằng chứng đó chỉ ra rằng những đảm bảo rằng sự giám sát chỉ được nhằm vào những người "đã làm gì đó không đúng" sẽ cung cấp ít sự thuận tiện, vì một nhà nước theo phản xạ sẽ coi bất kỳ thách thức nào đối với quyền lực của nó như là việc làm sai.

***

Các vụ việc những người nắm quyền qui cho những người chống đối chính trị như là "các mối đe dọa an ninh quốc gia" hoặc thậm chí "những tên khủng bố" được chứng minh một cách lặp lại là không thể cưỡng lại được. Trong thập kỷ vừa qua, chính phủ, trong sự đồng thanh với FBI của Hoover, đã chính thức chỉ định các nhà hoạt động môi trường như vậy, những mảng rộng của các nhóm cánh hữu chống chính phủ, các nhà hoạt động xã hội chống chiến tranh, và các hội đoàn được tổ chức xung quanh các quyền của người Palestin. Một số cá nhân nằm trong các chủng loại rộng lớn đó có thể xứng đáng với sự chỉ định đó, nhưng không nghi ngờ gì hầu hết mọi người thì không, tội lỗi chỉ vì việc giữ quan điểm chính trị đối nghịch. Vâng các nhóm như vậy thường bị ngắm đích đối với sự giám sát của NSA và các đối tác của nó.

Quả thực, sau khi các nhà chức trách nước Anh đã bỏ tù đối tác của tôi, David Miranda, ở sân bay Heathrow theo một đạo luật chống khủng bố, thì chính phủ Anh đã thể hiện ngang bằng với báo cáo giám sát của tôi về chủ nghĩa khủng bố trên cơ sở rằng sự phát hành các tài liệu của Snowden "được thiết kế để gây ảnh hưởng tới một chính phủ và được thực hiện vì các mục đích quảng bá một lý do chính trị hoặc tư tưởng". Điều này vì thế rơi vào trong định nghĩa của chủ nghĩa khủng bố. Đây là tuyên bố có khả năng rõ ràng nhất về việc kết nối một mối đe dọa tới lợi ích về quyền lực để chống chủ nghĩa khủng bố.

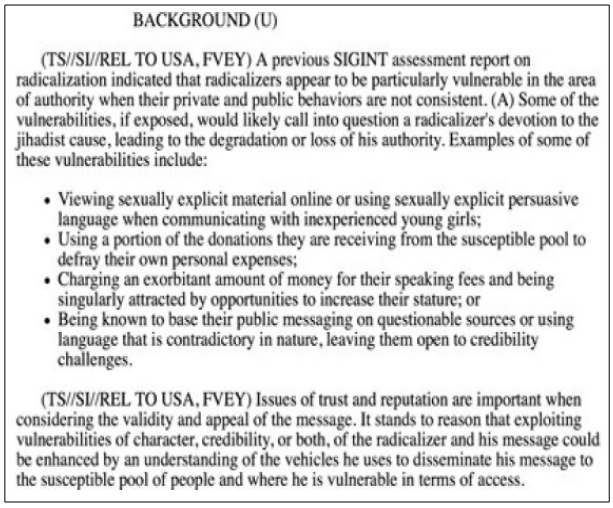
Không có gì về điều này có thể tới như là bất kỳ sự ngạc nhiên nào đối với cộng đồng những người Mỹ theo đạo Hồi, nơi mà nỗi sợ hãi giám sát trên cơ sở của chủ nghĩa khủng bố có cường độ mạnh và rộng khắp, và vì lý do tốt lành. Vào năm 2012, Adam Goldman và Matt Apuzzo của Associated Press đã tiết lộ một sơ đồ chung của Phòng Cảnh sát New York/CIA buộc toàn bộ các cộng đồng đạo Hồi ở nước Mỹ phải chịu sự giám sát vật lý và điện tử mà không quan tâm tới sự làm sai nào. Những người Mỹ theo đạo Hồi thường xuyên mô tả hiệu ứng gián điệp cuộc sống của họ: từng người mới mà nổi lên trong nhà thờ đạo Hồi được xem như là sự nghi ngờ về một người chỉ điểm của FBI; bạn bè và gia đình ngộp thở với các cuộc hội thoại của họ vì sợ đang bị giám sát và nằm ngoài nhận thức rằng bất kỳ quan điểm nào được thể hiện cũng được cho là thù địch với người Mỹ có thể được sử dụng như một cái cớ để điều tra hoặc thậm chí buộc tội.

Một tài liệu từ các hồ sơ của Snowden, đề ngày 03/10/2012, cay đắng nhấn mạnh điểm này. Nó đã tiết lộ rằng cơ quan này đã và đang giám sát các hoạt động trực tuyến của các cá nhân mà nó tin

tưởng thể hiện các ý tưởng "cơ bản" và những người có một ảnh hưởng "cơ bản hóa" tới những người khác. Bản ghi nhớ thảo luận về 6 cá nhân đặc biệt, tất cả là những người theo đạo Hồi, dù nó thể hiện rằng họ chỉ là "các mẫu ví dụ".

NSA rõ ràng nêu rằng không ai trong số các cá nhân bị ngắm đích là một thành viên của một tổ chức khủng bố hoặc có liên quan tới bất kỳ mưu đồ khủng bố nào. Thay vào đó, sự phạm tội của họ là quan điểm mà họ thể hiện, nó được coi là "cơ bản", một khái niệm mà đảm bảo cho sự giám sát rộng khắp và các chiến dịch tàn phá để "khai thác các chỗ bị tổn thương".

Trong số các thông tin thu thập được về các cá nhân, ít nhất một trong số họ là một "người Mỹ", là các chi tiết về các hoạt động tình dục trực tuyến và "tính hay chung chạ bừa bãi trên trực tuyến" - các site khiêu dâm mà họ viếng thăm và các cuộc chat tình dục lén lút với những phụ nữ mà không phải là vợ của họ. Cơ quan này thảo luận các cách thức để khai thác thông tin này để phá hủy các uy tín và sự tín nhiệm của họ.



BACKGROUND (U)

(TS//SI//REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particularly vulnerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these vulnerabilities include:

- Viewing sexually explicit material online or using sexually explicit persuasive language when communicating with inexperienced young girls;
- Using a portion of the donations they are receiving from the susceptible pool to defray their own personal expenses;
- Charging an exorbitant amount of money for their speaking fees and being singularly attracted by opportunities to increase their stature; or
- Being known to base their public messaging on questionable sources or using language that is contradictory in nature, leaving them open to credibility challenges.

(TS//SI//REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting vulnerabilities of character, credibility, or both, of the radicalizer and his message could be enhanced by an understanding of the vehicles he uses to disseminate his message to the susceptible pool of people and where he is vulnerable in terms of access.

Như phó giám đốc về pháp lý của ACLU, Jameel Jaffer, đã quan sát thấy, các cơ sở dữ liệu của NSA "lưu trữ thông tin về quan điểm chính trị của bạn, lịch sử y tế của bạn, các mối quan hệ mật thiết của bạn và các hoạt động trực tuyến của bạn". Cơ quan này nói thông tin cá nhân này sẽ không bị lạm dụng, "nhưng các tài liệu đó chỉ ra rằng NSA có thể xác định 'lạm dụng' rất hẹp". Như Jaffer đã chỉ ra, NSA về lịch sử, theo yêu cầu của một tổng thống, "đã sử dụng các kết quả giám sát để làm mất uy tín của đối thủ chính trị, nhà báo, hoặc nhà hoạt động xã hội về các quyền con người". Có lẽ là "ngây thơ", ông nói, để nghĩ cơ quan này còn không thể "sử dụng sức mạnh của mình theo cách đó".

Các tài liệu khác mô tả trọng tâm của chính phủ không chỉ vào WikiLeaks và người sáng lập của nó, Julian Assange, mà còn vào những gì cơ quan này gọi là "mạng những người ủng hộ WikiLeaks". Vào tháng 08/2010 chính quyền Obama đã thúc giục vài đồng minh đệ trình tố cáo có tội chống lại Assange vì xuất bản của nhóm này các lưu ký chiến tranh ở Afghanistan. Cuộc thảo luận xung quanh việc ép các quốc gia khác buộc tội Assange xuất hiện trong một hồ sơ của NSA mà cơ quan đó gọi nó là "*Dòng thời gian Săn người*" (*Manhunting Timeline*). Nó chi tiết hóa các đồng minh của

nó để định vị, khởi tố, bắt giữ và/hoặc giết các cá nhân khác nhau, trong số những người được cho là những tên khủng bố, buôn bán may túy, và các lãnh đạo Palestin. Một dòng thời gian cho từng năm giữa 2008 và 2012.

(U) Manhunting Timeline 2010

TOP SECRET//SI/TK//NOFORN

Jump to: navigation, search

Main article: Manhunting

See also: Manhunting Timeline 2011
See also: Manhunting Timeline 2009
See also: Manhunting Timeline 2008

(U) The following **manhunting operations took place in Calendar Year 2010**:

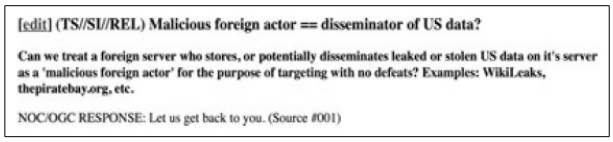
[edit] (U) November

Contents

[edit] (U) United States, Australia, Great Britain, Germany, Iceland

(U) The United States on 10 August urged other nations with forces in Afghanistan, including Australia, United Kingdom, and Germany, to consider filing criminal charges against Julian Assange, founder of the rogue Wikileaks Internet website and responsible for the unauthorized publication of over 70,000 classified documents covering the war in Afghanistan. The documents may have been provided to Wikileaks by Army Private First Class Bradley Manning. The appeal exemplifies the start of an international effort to focus the legal element of national power upon non-state actor Assange, and the human network that supports Wikileaks.[16]

Một tài liệu riêng rẽ có một tóm tắt về một trao đổi vào tháng 07/2011 về việc liệu WikiLeaks, cũng như website chia sẻ tệp Pirate Bay, có thể được chỉ định như là "một 'tác nhân nước ngoài độc hại' vì các mục đích ngắm đích hay không". Sự chỉ định có thể cho phép giám sát điện tử mở rộng các website đó, bao gồm cả những người sử dụng Mỹ. Thảo luận đó xuất hiện trong một danh sách "Các câu hỏi & đáp" (Q&A) theo đó các quan chức từ văn phòng Tuân thủ và Giám sát NTOC và Văn phòng Cố vấn Trưởng của NSA (NTOC Oversight and Compliance office (NOC) and NSA's Office of General Counsel (OGC)) cung cấp các câu trả lời cho các câu hỏi được đưa ra.

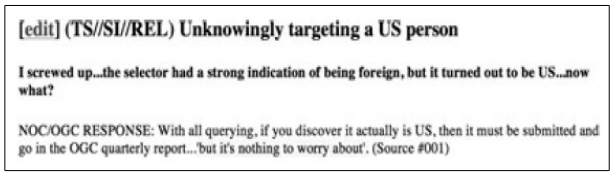


[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

Một trao đổi như vậy, từ năm 2011, đã chỉ ra sự bất phân biệt của NSA đối với việc vi phạm các qui định giám sát. Trong tài liệu, một thao tác viên nói, "tôi đã vặn", đã nhằm vào một người Mỹ thay vì một người nước ngoài. Câu trả lời từ văn phòng giám sát NSA và tổng cố vấn là, "chẳng có gì phải lo về điều đó".



[edit] (TS//SI//REL) Unknowingly targeting a US person

I screwed up...the selector had a strong indication of being foreign, but it turned out to be US...now what?

NOC/OGC RESPONSE: With all querying, if you discover it actually is US, then it must be submitted and go in the OGC quarterly report...'but it's nothing to worry about'. (Source #001)

Sự đối xử với nhóm Anonymous (Nặc danh), cũng như loại người mù mờ được biết như là "các tin tặc hoạt động xã hội" (hacktivist), là đặc biệt phiền toái và kỳ lạ. Đó là vì Anonymous thực sự là một nhóm có cấu trúc nhưng là một hội đoàn được tổ chức lỏng lẻo của những người xung quanh

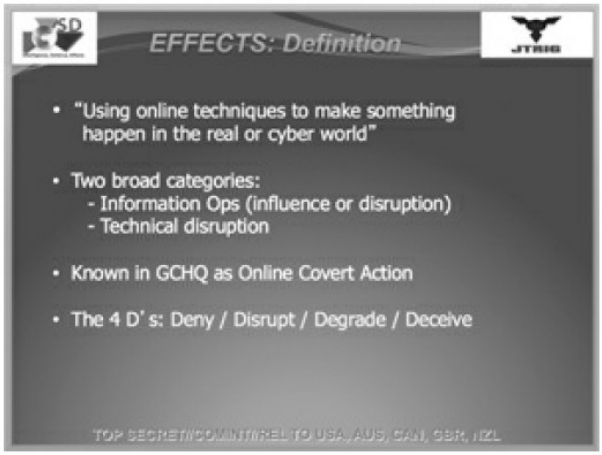
một ý tưởng: ai đó trở thành chi nhánh với Anonymous vì đức hạnh của các vị trí họ nắm giữ. Tệ hơn, chủng loại "hacktivist" không có nghĩa cố định: nó có thể có nghĩa là sử dụng các kỹ năng lập trình để làm xói mòn an ninh và việc vận hành của Internet nhưng cũng có thể tham chiếu tới bất kỳ ai sử dụng các công cụ trực tuyến để thúc đẩy các tư tưởng chính trị. NSA nhằm vào các loại rộng lớn những người tương đương với việc cho phép nó gián điệp bất kỳ ai bất kỳ ở đâu, bao gồm cả ở nước Mỹ, những ý tưởng của họ mà chính phủ thấy có đe dọa.

Gabriella Coleman, một chuyên gia về Anonymous ở Đại học McGill, nói rằng nhóm đó "không phải là một thực thể xác định" mà thay vào đó là "một ý tưởng động viên được các nhà hoạt động xã hội tiến hành hành động hợp tác và lên tiếng về sự không hài lòng về chính trị. Đây là một phong trào xã hội toàn cầu có trụ sở ở khắp nơi mà không có cấu trúc lãnh đạo tập trung hoặc được tổ chức một cách chính thống. Một số đã tập hợp lại xung quanh cái tên này để tham gia vào sự bất tuân dân sự số, nhưng chẳng có gì giống dù là xa với chủ nghĩa khủng bố".

Đa số những người ôm lấy ý tưởng đó đã tiến hành "trước hết vì sự thể hiện chính trị thông thường. Việc nhằm vào Anonymous và các hacktivist được coi như việc nhằm vào các công dân thể hiện lòng tin chính trị của họ, gây ra sự ngột ngạt đối với sự bất đồng chính kiến hợp pháp", Coleman đã giải thích.

Vâng Anonymous từng bị một đơn vị của GCHQ ngắm đích bằng việc sử dụng một số chiến thuật cơ bản và gây tranh cãi nhất được biết tới như là spycraft: "các hoạt động cắm cờ sai", "các cái bẫy đường mật", các virus và các cuộc tấn công khác, các chiến lược lừa gạt nghi binh, và "các lựa chọn thông tin để làm hại uy tín".

Một slide PowerPoint được các quan chức giám sát của GCHQ trình chiếu trong hội nghị SigDev 2012 mô tả 2 dạng tấn công: "các lựa chọn thông tin (gây ảnh hưởng hoặc phá hủy)" và "phá hủy kỹ thuật". GCHQ tham chiếu tới các biện pháp đó như là "Hành động Giấu giếm Trực tuyến", nó có ý định để đạt được những gì tài liệu gọi là "4D: Từ chối/Phá hủy/Làm thoái hóa/Lừa gạt nghi binh" (Deny/Disrupt/Degrade/Deceive).

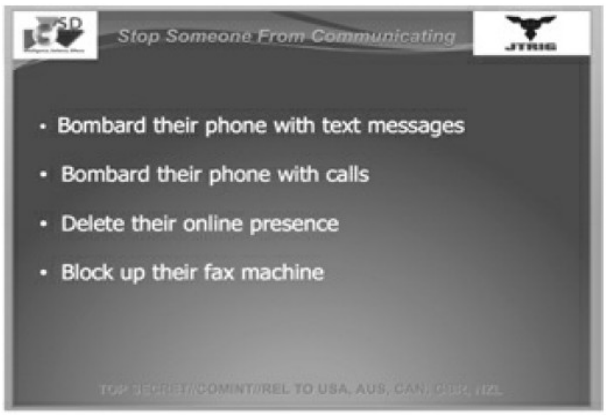


Một slide khác mô tả các chiến thuật được sử dụng để "làm mất uy tín của đối tượng đích". Chúng

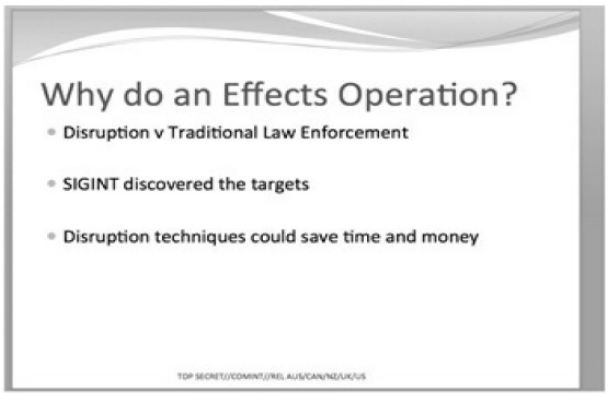
bao gồm "thiết lập một cái bẫy đường mật", "thay đổi các hình ảnh trong các site kết nối mạng xã hội", "viết một blog có mục đích là một trong các nạn nhân của chúng", và "gửi thư điện tử/văn bản cho các đồng nghiệp, hàng xóm, bạn bè của họ, ..."

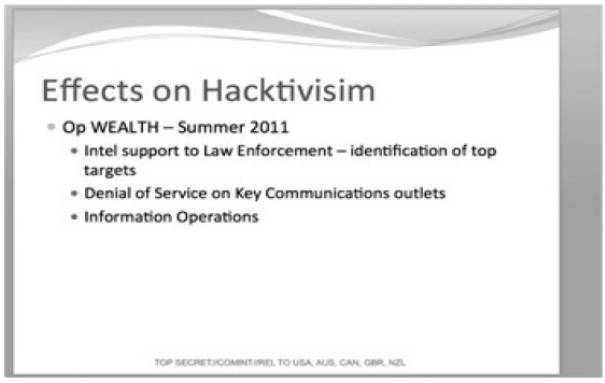
Đi kèm với các lưu ý, GCHQ giải thích rằng "cái bẫy đường mật" - một chiến thuật thời Chiến tranh Lạnh xưa cũ có liên quan tới việc sử dụng các phụ nữ quyến rũ để nhử các mục tiêu nam giới vào trong các tình huống làm tổn thương, làm mất uy tín - đã và đang được cập nhật cho kỷ nguyên số: bây giờ một cái đích được nhử làm tổn thương một site hoặc sự gặp gỡ trực tuyến. Bình luận được bổ sung thêm: "một lựa chọn lớn. Rất thành công khi nó làm việc". Tương tự, các phương pháp thâm nhập nhóm theo truyền thống bây giờ được thực hiện trực tuyến:

Một kỹ thuật khác có liên quan tới việc dừng "ai đó khỏi việc giao tiếp". Để làm thế, cơ quan này sẽ "bỏ bom điện thoại của họ bằng các thông điệp văn bản", "bỏ bom điện thoại của họ bằng các cuộc gọi", "xóa sự hiện diện trực tuyến của họ", và "khóa máy fax của họ lại".



GCHQ cũng thích sử dụng các kỹ thuật "phá hủy" trong số những gì nó gọi là "ép tuân thủ luật theo truyền thống" như việc thu thập bằng chứng, các tòa án, và các khởi tố. Trong một tài liệu có đầu đề "Phiên Tấn công Không gian mạng: Thúc đẩy các đường biên và hành động chống lại Hacktivism", GCHQ thảo luận việc ngắm đích của nó đối với các "hacktivist" với, thật trớ trêu, các cuộc tấn công "từ chối dịch vụ", một chiến thuật thường có liên quan tới các tin tặc:



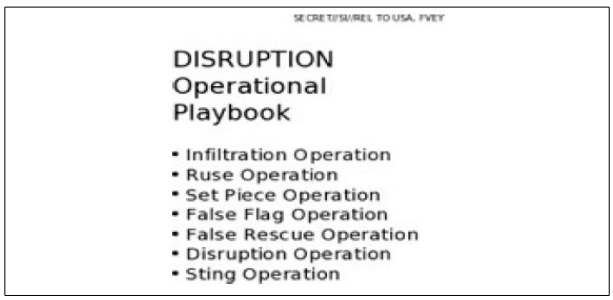


Cơ quan giám sát của nước Anh cũng sử dụng một đội các nhà khoa học xã hội, bao gồm cả các nhà tâm lý học, để phát triển các kỹ thuật "tình báo con người trực tuyến" - Online HUMINT (human intelligence) và "phá hoại ảnh hưởng chiến lược". Tài liệu "Nghệ thuật Lừa gạt nghi binh: Huấn luyện cho một Thế hệ Mới các Tác chiến Giấu giếm Trực tuyến" được dành cho các chiến thuật đó. Được Trung tâm Tác chiến Khoa học Con người - HSCO (Human Science Operation Cell) chuẩn bị, tài liệu nói thiết kế trong các lĩnh vực xã hội học, tâm lý học, nhân chủng học, khoa học thần kinh, và sinh vật học, và các lĩnh vực khác, để tối đa hóa các kỹ năng lừa gạt nghi binh của GCHQ.

Một slide chỉ ra cách tham gia vào "Ngụy trang - Ẩnh và Hiện", trong khi tuyên truyền "Sự mô phỏng - Chỉ ra sự Sai trái". Nó kiểm tra "các khối nhà tâm lý học lừa gạt nghi binh" và "bản đồ các công nghệ" được sử dụng để triển khai các lừa gạt nghi binh, bao gồm cả Facebook, Twitter, LinkedIn, và "các trang web".

Việc nhấn mạnh rằng "mọi người ra các quyết định vì những lý do tình cảm chứ không phải vì các lý do dựa vào lý trí", GCHQ tranh luận rằng hành vi trực tuyến được dẫn dắt bởi "việc soi gương" ("mọi người sao chụp lẫn nhau trong lúc tương tác xã hội với chúng"), "điều tiết thích nghi" và "bắt chước" ("sự áp dụng các nét đặc biệt của người giao tiếp từ người tham gia khác").

Tài liệu sau đó đưa ra những gì nó gọi là "Sách chơi Hoạt động Phá hoại" (Disruption Operational Playbook). Điều này bao gồm "hoạt động thâm nhập", "hoạt động dùng mưu", "hoạt động cắm cờ sai", "hoạt động làm đau". Nó thể một "sự triển khai đầy đủ" chương trình phá hoại "tới đầu năm 2013" khi "hơn 150 nhân viên được huấn luyện đầy đủ".



Dưới đầu đề "Các kỹ thuật và Kinh nghiệm kỳ diệu", tài liệu tham chiếu tới "Sự hợp pháp hóa vi phạm", "Việc xây dựng kinh nghiệm trong tâm trí về các mục tiêu sẽ được chấp nhận sao cho chúng sẽ không hiện thực hóa được" và "Việc tối ưu hóa các kênh lừa gạt nghi binh".

Các kế hoạch như vậy của chính phủ để giám sát và gây ảnh hưởng tới các giao tiếp truyền thông Internet và phổ biến các thông tin sai lệch trên trực tuyến đã từ lâu là một nguồn suy đoán. Giáo sư luật của Đại học Harvard Cass Sunstein, một cố vấn thân cận của Obama, cựu lãnh đạo của Văn phòng Thông tin và các Công việc Điều chỉnh của Nhà Trắng, và là một người được chỉ định cho nhóm của Nhà Trắng để rà soát lại các hoạt động của NSA, đã viết một tài liệu gây tranh cãi trong năm 2008 đề xuất rằng chính phủ Mỹ sử dụng các đội các đặc vụ giấu giếm và những người bảo vệ "độc lập" giả cho "sự thâm nhập dựa vào sự hiểu biết" của các nhóm trực tuyến, các phòng chat, các mạng xã hội, và các website, cũng như các nhóm hoạt động xã hội phi trực tuyến.

Các tài liệu của GCHQ chỉ ra lần đầu tiên rằng các kỹ thuật gây tranh cãi đó để lừa gạt nghi binh và làm tổn hại uy tín đã chuyển từ giai đoạn đề xuất sang triển khai.

***

Tất cả các bằng chứng nhấn mạnh sự mặc cả ngầm được chào cho các công dân: không đặt ra thách thức và bạn không có gì để mà lo lắng. Hãy để tâm tới việc kinh doanh của riêng bạn, và ủng hộ hoặc ít nhất chịu đứng những gì chúng tôi làm, và bạn sẽ OK. Đặt khác đi, bạn phải kiềm chế kích động nhà chức trách mà nắm sức mạnh giám sát nếu bạn muốn được coi là không làm những việc sai trái. Đây là một vụ làm ăn mà nó mời tính tiêu cực, sự phục tùng và sự tuân thủ. Tiến trình nhanh nhất, cách để đảm bảo "được để yên lại một mình", là giữ im lặng, nín thở, và tuân thủ.

Đối với nhiều người, vụ làm ăn này là quyến rũ, thuyết phục đa số rằng sự giám sát là nhân từ hoặc thậm chí có lợi. Họ đang quá chán phải lôi cuốn sự chú ý của chính phủ, họ suy luận.

"Tôi nghiêm túc nghi ngờ rằng NSA có quan tâm tới tôi" là dạng điều mà tôi thường nghe. "Nếu họ muốn nghe theo cuộc sống chán nản của tôi, thì họ được chào đón". Hoặc "NSA không quan tâm tới việc nói chuyện của bà của bạn về các hóa đơn của bà hoặc việc lên kế hoạch của bố bạn cho trò chơi golf của ông".

Đó là những người mà đã trở nên bị thuyết phục rằng bản thân họ sẽ không bị ngắm đích cá nhân - vì họ đang không đe dọa và họ đang tuân thủ - và vì thế hoặc từ chối điều sẽ xảy ra, không quan tâm, hoặc có thiện chí ủng hộ nó một cách dứt khoát.

Khi phỏng vấn tôi ngay khi câu chuyện của NSA vỡ lở, Lawrence O'Donnell của chủ nhà MSNBC đã chế giễu khái niệm của NSA như là "một con quái vật giám sát to lớn, đáng sợ". Tóm tắt quan điểm của ông, ông đã kết luận:

> Cảm giác của tôi cho tới nay là... Tôi không sợ... thực tế là chính phủ đang thu thập [dữ liệu] ở mức độ khủng khiếp, khổng lồ có nghĩa là thậm chí còn khó khăn hơn cho chính phủ để tìm ra tôi... và họ tuyệt đối không có động lực để tìm ra tôi. Và vì thế tôi, ở giai đoạn này, cảm thấy hoàn toàn không bị điều này đe dọa.

Hendrik Hertzberg của tờ *New York Times* cũng đã khẳng định quan điểm tùy tiện tương tự về các mối nguy hiểm của giám sát. Thừa nhận rằng có "các lý do để quan tâm về sự quá xá của cơ quan tình báo, sự bí mật quá xá, và thiếu minh bạch", ông đã viết rằng "cũng có các lý do để giữ được

bình yên", đặc biệt, rằng mối đe dọa được đặt ra "cho các quyền tự do dân sự, như nó là, là trừu tượng, phỏng đoán, không xác định". Và người chịu trách nhiệm về chuyên mục của tờ *Washington Post* Ruth Marcus, làm giảm giá trị mối quan tâm về sức mạnh của NSA, đã tuyên bố - lố bịch - "siêu dữ liệu của tôi hầu như chắc chắn đã không bị soi xét kỹ lưỡng".

Theo một ý nghĩa quan trọng, O'Donnell, Hertzberg và Marcus là đúng. Đó là trường hợp mà chính phủ Mỹ "tuyệt đối không có sự khuyến khích" để nhằm vào những người như họ, đối với những người mà mối đe dọa từ một nhà nước giám sát là ít hơn so với "trừu tượng, phỏng đoán, không xác định". Điều đó giải thích vì sao các nhà báo mà hiến dâng sự nghiệp của họ cho việc tôn thờ quan chức có sức mạnh nhất của đất nước - tổng thống, người là tổng chỉ huy của NSA - và hiếm khi bảo vệ đảng chính trị của ông ta, nếu bao giờ đó có, mạo hiểm xa lánh những người có sức mạnh.

Tất nhiên, những người ủng hộ trung thành và biết nghe lời tổng thống và các chính sách của ông ta, các công dân tốt, những người không làm gì để thu hút sự chú ý tiêu cực từ sự quyền thế, không có lý do gì để sợ nhà nước giám sát. Đây là trường hợp trong mọi xã hội: những người không đặt ra thách thức sẽ hiếm khi bị ngắm đích bởi những biện pháp đàn áp, và từ quan điểm của họ, họ có thể sau đó thuyết phục bản thân họ rằng sự đàn áp thực sự không tồn tại. Nhưng biện pháp đúng đối với tự do của xã hội là cách mà nó đối xử với những người bất đồng chính kiến của nó và các nhóm bị thiệt thòi khác, chứ không phải cách mà nó đối xử với những người trung thành tốt. Thậm chí trong những chính thể chuyên chế tồi tệ nhất thế giới, những người ủng hộ biết vâng lời sẽ được miễn dịch đối với các lạm dụng của sức mạnh nhà nước. Tại Ai cập của Mubarak, chính là những người từng xuống đường để làm rung chuyển vì sự lật đổ ông ta, những người đã từng bị bắt bớ, bị tra tấn, bị bắn hạ; những người ủng hộ Mubarak và những người mà âm thầm nằm lại ở nhà đã không. Tại nước Mỹ, đó từng là các nhà lãnh đạo của NAACP, những người cộng sản, và các nhà hoạt động xã hội chống chiến tranh và các quyền dân sự, những người từng bị ngắm đích với sự giám sát của Hoover, không phải các công dân hành xử tốt mà giữ câm lặng về sự bất công của xã hội.

Chúng ta sẽ không phải là những tôi trung đáng tin cậy của quyền lực để cảm thấy an toàn đối với sự giám sát của nhà nước. Cái giá của sự miễn dịch cũng không phải là việc kìm hãm đối với sự bất đồng chính kiến gây tranh cãi hoặc đầy khiêu khích.

Chúng ta không muốn một xã hội nơi mà thông điệp được truyền đạt rằng bạn sẽ được để yên lại một mình chỉ nếu bạn bắt chước hành vi thuận tiện và sự khôn ngoan thường thấy của một nhà báo có tiếng.

Vượt ra khỏi điều đó, ý nghĩa của sự miễn dịch được một nhóm đặc biệt cảm thấy hiện hành có sức mạnh bị ràng buộc sẽ là hão huyền viển vông. Điều được làm rõ khi chúng ta nhìn vào cách mà hội đoàn đảng phái định hình ý thức về các mối nguy hiểm của mọi người đối với sự giám sát của nhà nước. Điều nổi lên là việc những người cổ vũ của ngày hôm qua có thể nhanh chóng trở thành những người bất đồng chính kiến của ngày hôm nay.

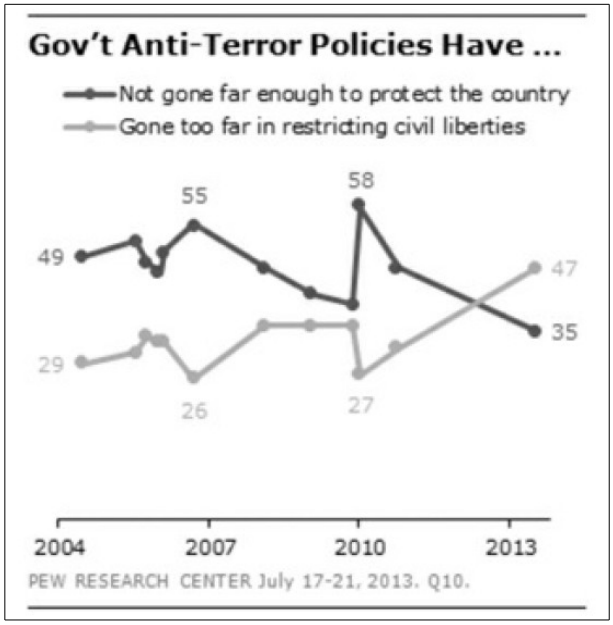
Vào thời điểm năm 2005 đối với sự tranh cãi nghe lén không có lệnh cho phép của NSA, những người theo chủ nghĩa tự do và các đảng viên đang Dân chủ đã coi một cách áp đảo chương trình giám sát của cơ quan đó như là sự hăm dọa. Tất nhiên, một phần của điều này từng là chiếc xe 2

bánh điển hình của đảng: George W. Bush từng là tổng thống và những người của đảng Dân chủ đã thấy một cơ hội để giáng thiệt hại chính trị lên ông ta và đảng của ông ta. Nhưng một phần đáng kể của nỗi sợ hãi của họ từng có thực: vì họ đã coi Bush là độc hại và nguy hiểm, họ đã nhận thấy rằng giám sát nhà nước dưới sự kiểm soát của ông ta vì thế từng đe dọa và rằng họ đặc biệt từng gặp nguy hiểm như là các đối thủ chính trị. Vì vậy, những người của đảng Cộng hòa đã có quan điểm lành tính hoặc ủng hộ hơn các hành động của NSA. Vào tháng 12/2013, ngược lại, những người của đảng Dân chủ và những người tiến bộ đã trở thành những người bảo vệ hàng đầu của NSA.

Các dữ liệu thăm dò ý kiến rộng rãi đã phản ánh sự dịch chuyển này. Vào cuối tháng 07/2013, Trung tâm Nghiên cứu Pew đã đưa ra một thăm dò ý kiến chỉ ra rằng đa số những người Mỹ đã không còn tin vào những phòng thủ bảo vệ được đưa ra cho các hành động của NSA nữa. Đặc biệt, "đa số những người Mỹ - 56% - nói rằng các tòa án liên bang thất bại để đưa ra những hạn chế phù hợp về dữ liệu điện thoại và Internet mà chính phủ đang thu thập như một phần của các nỗ lực chống khủng bố của nó". Và "thậm chí một tỷ lệ còn lớn hơn (70%) tin tưởng rằng chính phủ sử dụng các dữ liệu này cho những mục đích khác so với việc điều tra khủng bố". Hơn nữa, "63% nghĩ chính phủ cũng đang thu thập thông tin về nội dung các giao tiếp truyền thông".

Đáng lưu ý nhất, những người Mỹ bây giờ đã coi sự nguy hiểm của giám sát như là mối lo lớn hơn so với sự nguy hiểm của chủ nghĩa khủng bố:

> Tổng thể, 47% nói lo lắng lớn hơn của họ về các chính sách chống khủng bố của chính phủ là họ đã đi quá xa trong việc hạn chế các quyền tự do dân sự của người bình thường, trong khi 35% nói họ có quan tâm hơn rằng các chính sách đã không đi đủ xa để bảo vệ đất nước. Đây là lần đầu tiên trong thăm dò ý kiến của Pew Research mà nhiều người hơn đã thể hiện sự quan tâm của họ về các quyền tự do dân sự hơn là sự bảo vệ khỏi chủ nghĩa khủng bố kể từ khi câu hỏi này được đưa ra lần đầu tiên vào năm 2004.



Các dữ liệu thăm dò ý kiến đó từng là tin tức tốt lành cho bất kỳ ai bị sự sử dụng quyền lực quá xá của chính phủ và sự thổi phồng kinh niên về mối đe dọa khủng bố cảnh báo. Nhưng nó đã nhấn mạnh một sự nói đảo ngược: Những người của đảng Cộng hòa, những người từng bảo vệ NSA dưới thời Bush, từng bị những người của đảng Dân chủ hất cẳng khi hệ thống giám sát đã trở thành nằm dưới sự kiểm soát của Tổng thống Obama, một trong những người của riêng họ. "Toàn thể đất nước, có sự ủng hộ hơn cho chương trình thu thập dữ liệu của chính phủ trong số những người của đảng Dân chủ (57% phê chuẩn) so với trong số những người của đảng Cộng hòa (44%)".

Các dữ liệu thăm dò ý kiến tương tự từ tờ *Washington Post* đã tiết lộ rằng những người bảo thủ từng lo lắng nhiều hơn nhiều về việc gián điệp của NSA so với những người theo chủ nghĩa tự do. Khi được hỏi, "bạn có quan tâm như thế nào, nếu trong tất cả, về sự thu thập và sử dụng thông tin cá nhân của bạn từ Cơ quan An ninh Quốc gia?" 48% những người bảo thủ từng "rất có quan tâm" so với chỉ 26% những người theo chủ nghĩa tự do. Như giáo sư luật Orin Kerr đã lưu ý, điều này đã đại diện cho một sự thay đổi cơ bản: "Đây là một sự lộn ngược thú vị từ năm 2006, khi Tổng thống từng là một người của đảng Cộng hòa thay vì một người của đảng Dân chủ. Ngược về khi đó, một cuộc thăm dò ý kiến của Peww đã thấy 75% những người của đảng Cộng hòa đã phê chuẩn sự giám sát của NSA nhưng chỉ 37% những người của đảng Dân chủ đã phê chuẩn".

Một đồ thị của Pew tạo sự dịch chuyển rõ ràng:

Partisan Shifts in Views of NSA Surveillance Programs

Views of NSA surveillance programs
(See previous table for differences in question wording)

	January 2006		June 2013	
	Accept-able	Un-acceptable	Accept-able	Un-acceptable
	%	%	%	%
Total	51	47	56	41
Republican	75	23	52	47
Democrat	37	61	64	34
Independent	44	55	53	44

PEW RESEARCH CENTER June 6-9, 2013. Figures read across. Don't know/Refused responses not shown.

Những lý lẽ theo và chống sự giám sát xoay chuyển một cách trơ trẽn, dựa vào đảng nào nắm quyền. Sự thu thập cả đống siêu dữ liệu từng được nêu một cách áp đảo từ một thượng nghị sỹ vào đầu của The Early Show vào năm 2006 theo cách này:

> Tôi không phải nghe các cuộc gọi điện thoại của bạn để biết những gì bạn đang làm. Nếu tôi biết từng cuộc gọi điện thoại mà bạn thực hiện, thì tôi có khả năng xác định từng người mà bạn đã nói chuyện với. Tôi có thể có được một mẫu về cuộc sống của bạn mà là rất, rất bừa bãi... Và câu hỏi thực sự ở đây là: Họ làm gì với thông tin này mà họ thu thập mà không có gì để làm với Al Qaeda?... Và chúng ta sẽ tin cậy tổng thống và phó tổng thống

của nước Mỹ rằng họ đang làm điều đúng phải không? Đừng có tính tôi trong số đó.

Thượng nghị sỹ đang tấn công cực kỳ cay nghiệt sự thu thập siêu dữ liệu đó từng là Joe Biden, người sau này, như là phó tổng thống, đã trở thành một phần của một chính quyền của đảng Dân chủ, mà đã đưa ra chính xác những lý lẽ y hệt mà ông ta đã từng chế nhạo.

Điểm phù hợp ở đây không chỉ đơn thuần rằng nhiều người trung thành của đảng là những kẻ đạo đức giả bất lương với những thuyết phục không thực tế khác với một đòi hỏi về quyền lực, dù điều đó chắc chắn là đúng. Quan trọng hơn là những gì các tuyên bố như vậy tiết lộ về bản chất tự nhiên của cách một người nhìn sự giám sát nhà nước. Như với quá nhiều sự bất công, mọi người có thiện chí bỏ qua nỗi sợ hãi đối với sự đi quá xa của chính phủ khi họ tin tưởng rằng họ, những người bỗng nhiên nắm sự kiểm soát sẽ nhân từ và đáng tin cậy. Họ xem sự giám sát là nguy hiểm hoặc đang mang theo chỉ khi họ hiểu được rằng bản thân họ bị điều đó đe dọa.

Những mở rộng quyền lực triệt để tận gốc thường được đưa ra theo cách này, bằng việc thuyết phục mọi người rằng chúng chỉ ảnh hưởng tới một nhóm đặc thù, riêng biệt. Các chính phủ từ lâu đã thuyết phục dân chúng nhắm mắt làm ngơ để tiến hành đàn áp bằng việc dẫn dắt các công dân để tin tưởng, dù đúng hay sai, rằng chỉ những người nhất định bị thiệt thòi là bị ngắm đích, và mỗi người nào đó khác có thể bằng lòng hoặc thậm chí ủng hộ sự đàn áp đó mà không sợ rằng nó sẽ được áp dụng cho chính họ. Để sang một bên những khiếm khuyết rõ ràng về đạo đức của trạng thái này - chúng ta không bỏ qua chủ nghĩa phân biệt chủng tộc vì nó được định hướng vào thiểu số, hoặc nhún vai coi khinh sự đói kém trên trái đất khi chúng ta hưởng thụ một sự cung cấp thực phẩm dồi dào sung túc - điều hầu như luôn bị nhầm đường lạc lối trong các nền tảng thực dụng.

Sự thờ ơ hoặc ủng hộ những người nghĩ bản thân họ được miễn bất kỳ lúc nào sẽ cho phép sử dụng sai quyền lực để lan truyền vượt ra xa hơn nhiều sự áp dụng ban đầu của nó, cho tới khi sự lạm dụng trở thành không có khả năng để kiểm soát - nhưng nó sẽ không thể tránh khỏi thế. Có quá nhiều ví dụ để tính tới, nhưng có lẽ ví dụ mạnh mẽ và gần đây nhất là sự khai thác Luật Yêu nước (Patriot Act). Một Quốc hội gần như hoàn toàn nhất trí đã phê chuẩn một sự gia tăng ồ ạt trong quyền lực giám sát và bắt giữ sau ngày 11/09, bị thuyết phục vì lý lẽ rằng làm như thế có thể dò tìm ra và ngăn chặn được các cuộc tấn công trong tương lai.

Giả thiết ngầm rằng quyền lực có thể được sử dụng chủ yếu chống lại đạo Hồi trong mối liên quan tới chủ nghĩa khủng bố - một sự mở rộng kinh điển quyền lực được bó trong một nhóm đặc biệt được giữ trước ở một dạng hành động đặc biệt - là một lý do giải thích vì sao biện pháp đó đã nhận được sự ủng hộ áp đảo. Nhưng những gì đã diễn ra từng là rất khác: Luật Yêu nước từng được áp dụng tốt vượt ra khỏi mục đích được che đậy bên ngoài của nó. Trong thực tế, kể từ khi nó được ban hành, nó từng được sử dụng một cách áp đảo trong các trường hợp không có điều gì hoàn toàn để làm với chủ nghĩa khủng bố hoặc an ninh quốc gia. Tạp chí *New York* đã tiết lộ rằng từ 2006 tới 2009, điều khoản "lẻn vào và hé nhìn" của luật (cấp phép để thực thi một lệnh tìm kiếm mà ngay lập tức không thông báo cho mục tiêu đích) từng được sử dụng trong 1.618 vụ việc có liên quan tới

ma túy, 122 vụ việc liên quan tới hàng giả, và chỉ 15 vụ việc liên quan tới chủ nghĩa khủng bố.

Nhưng một khi toàn thể công dân bằng lòng với một quyền lực mới, tin tưởng rằng nó không ảnh hưởng tới họ, thì nó đã trở thành được thể chế hóa và được hợp pháp hóa và sự chống đối đã trở nên không thể. Quả thực, bài học trọng tâm mà Frank Church học được trong năm 1975 từng là mức độ nguy hiểm do sự giám sát ồ ạt đã đặt ra. Trong một cuộc phỏng vấn trên Meet the Press (gặp gỡ báo chí), ông nói:

> Khả năng bất kỳ lúc nào cũng có thể được chuyển tới xung quanh người dân Mỹ và không người Mỹ nào có thể có bất kỳ tính riêng tư nào được để lại, khả năng như vậy để theo dõi bất kỳ điều gì - các cuộc hội thoại điện thoại, các bức điện tín, không thành vấn đề. Có thể sẽ không có nơi nào để ẩn nấp. Nếu chính phủ này lúc nào đó trở thành một bạo chúa... thì khả năng công nghệ mà cộng đồng tình báo có được trao cho chính phủ có thể cho phép nó áp đặt toàn bộ sự bạo ngược, và có thể không có cách gì để đánh lại vì nỗ lực thận trọng nhất để kết hợp cùng nhau trong sự phản kháng ... nằm trong tầm với của chính phủ để biết được. Khả năng của công nghệ đó là như vậy.

Viết trên New York Times vào năm 2005, James Bamford đã quan sát thấy rằng mối đe dọa từ giám sát nhà nước là thảm khốc hơn nhiều ngày nay so với nó từng có trong những năm 1970:

"Với những người biểu lộ các suy nghĩ tận đáy lòng của họ trong các thông điệp thư điện tử, việc mở ra các hồ sơ y tế và tài chính của họ tới Internet, và việc chat tức thì trong các điện thoại cầm tay, cơ quan đó hầu như có khả năng để nằm bên trong trí óc của một con người".

Mối lo ngại của Church, rằng bất kỳ khả năng giám sát nào "cũng có thể được chuyển tới xung quanh người dân Mỹ", chính xác là những gì NSA đã làm sau ngày 11/09. Bất chấp việc vận hành theo Luật Giám sát Tình báo Nước ngoài - FISA (Foreign Intelligence Surveillance Act), và bất chấp sự cấm chỉ trong việc gián điệp nội địa được nhúng vào nhiệm vụ của cơ quan đó từ đầu, nhiều trong số các hoạt động giám sát của nó bây giờ tập trung vào các công dân Mỹ trên đất Mỹ.

Thậm chí thiếu vắng sự lạm dụng, và thậm chí nếu một người không bị ngắm đích một cách riêng rẽ cá nhân, thì một nhà nước giám sát mà việc thu thập tất cả của nó làm hại cho xã hội và sự tự do chính trị nói chung. Sự tiến bộ cả ở nước Mỹ và các quốc gia khác từng chỉ đạt được từ trước tới nay thông qua khả năng thách thức quyền lực và tính chính thống và để tiên phong mở ra các con đường tư duy và sống động mới. Mỗi người, thậm chí những người mà không tham gia vào việc bảo vệ bất đồng chính kiến hoặc hoạt động xã hội chính trị, phải chịu đựng khi quyền tự do đó bị bóp nghẹt vì nỗi sợ hãi đang bị theo dõi. Hendrik Hertzberg, người đã đánh giá thấp các mối lo ngại về các chương trình của NSA, dù sao cũng đã thừa nhận rằng "sự thiệt hại đã được thực hiện. Sự thiệt hại là dân sự. Sự thiệt hại là tập thể. Sự thiệt hại là đối với kiến trúc của lòng tin và trách nhiệm giải trình mà hỗ trợ cho một xã hội cởi mở và một chính thể dân chủ".

***

Những người cổ vũ giám sát về cơ bản chỉ đưa ra một lý lẽ bảo vệ sự giám sát ồ ạt: nó chỉ được triển khai để dừng chủ nghĩa khủng bố và giữ cho mọi người an toàn. Quả thực, việc viện tới một

mối đe dọa bên ngoài là một chiến thuật lựa chọn lịch sử để giữ cho dân chúng phục tùng quyền lực của chính phủ. Chính phủ Mỹ đã báo trước sự nguy hiểm của chủ nghĩa khủng bố từ hơn một thập kỷ để minh chứng cho một đống các hành động cơ bản, từ sự bỏ tù và tra tấn tới ám sát và xâm lược Iraq. Kể từ cuộc tấn công ngày 11/09, các quan chức Mỹ theo phản xạ tạo ra từ "chủ nghĩa khủng bố". Nó là xa hơn nhiều một khẩu hiệu và chiến thuật so với một lý lẽ thực sự hoặc sự minh chứng có sức thuyết phục để hành động. Và trong trường hợp của sự giám sát, bằng chứng áp đảo chỉ ra sự minh chứng là mơ hồ như thế nào.

Để bắt đầu, nhiều sự thu thập dữ liệu được NSA tiến hành hiển nhiên không có gì phải làm với chủ nghĩa khủng bố hoặc an ninh quốc gia. Việc can thiệp các giao tiếp truyền thông của người khổng lồ dầu khí Petrobras của Brazil hoặc việc gián điệp các phiên thương thảo ở một hội nghị thượng đỉnh về kinh tế hoặc việc ngắm đích các lãnh đạo được bầu một cách dân chủ của các quốc gia đồng minh hoặc việc thu thập các hồ sơ giao tiếp truyền thông của tất cả những người Mỹ đều không có mối quan hệ nào với chủ nghĩa khủng bố cả. Biết rằng sự giám sát thực tế mà NSA làm, dừng khủng bố rõ ràng là một sự viện cớ.

Hơn nữa, lý lẽ rằng sự giám sát ồ ạt đã ngăn chặn được các âm mưu khủng bố - một tiếng kêu được Tổng thống Obama và một loạt các nhân vật về an ninh quốc gia đưa ra - đã được chứng minh là sai. Như tờ *Washington Post* đã lưu ý hồi tháng 12/2013, trong một bài báo có đầu đề "Bảo vệ chương trình điện thoại của NSA của các quan chức có thể làm sáng tỏ", một thẩm phán liên bang đã tuyên bố chương trình thu thập siêu dữ liệu điện thoại "hầu như chắc chắn" là vi hiến, trong quá trình nói rằng Bộ Tư pháp đã thất bại để "trích dẫn một trường hợp duy nhất trong đó sự phân tích việc thu thập đống siêu dữ liệu của NSA thực sự đã làm dừng một cuộc tấn công khủng bố sắp tới".

Cùng tháng đó, nhóm cố vấn được Obama nhặt ra bằng tay (bao gồm, trong số những người khác, một cựu phó giám đốc CIA và một cựu sĩ quan phụ tá của Nhà Trắng, và được triệu tập để nghiên cứu chương trình của NSA thông qua sự truy cập tới các thông tin bí mật) đã kết luận rằng chương trình siêu dữ liệu "từng không là cơ bản cho việc ngăn chặn các cuộc tấn công và có thể đã giành được rồi theo một cách thức đúng lúc bằng việc sử dụng các lệnh theo qui ước [của tòa án]".

Trích dẫn tờ *Washington Post* một lần nữa: "Trong lời chứng trước quốc hội, [Keith] Alexander đã công nhận chương trình với việc trợ giúp dò tìm ra hàng tá các âm mưu cả trong nước Mỹ và ở nước ngoài" nhưng báo cáo của nhóm cố vấn "đã cắt đi sâu sắc độ tin cậy của những tuyên bố đó".

Hơn nữa, như các thượng nghị sỹ của đảng Dân chủ Ron Wyden, Mark Udall, và Martin Heinrich - tất cả các thành viên của Ủy ban Tình báo - đã tuyên bố thẳng thắn trên tờ *New York Times*, sự thu thập ồ ạt các bản ghi điện thoại đã không cải thiện được sự bảo vệ những người Mỹ khỏi mối đe dọa của chủ nghĩa khủng bố.

> Sự vô dụng của chương trình thu thập cả đống đã từng được phóng đại quá mức. Chúng tôi vẫn chưa thấy bất kỳ bằng chứng nào chứng minh rằng nó đưa ra giá trị thực sự, có một không hai trong việc bảo vệ an ninh quốc gia. Bất chấp các yêu cầu lặp đi lặp lại của chúng tôi, NSA đã không đưa ra được bằng chứng về bất kỳ trường hợp nào khi cơ quan đó đã sử dụng chương trình này để rà soát lại các bản ghi điện thoại mà có thể đã không giành được

bằng việc sử dụng một lệnh tòa án thông thường hoặc quyền khẩn cấp.

Một nghiên cứu của người có chủ trương ôn hòa *Quỹ nước Mỹ Mới* (*New America Foundation*) kiểm thử tính chân thực các minh chứng của các quan chức cho sự thu thập cả đống siêu dữ liệu đã đồng ý rằng chương trình đó "đã không có tác động nào có thể thấy rõ về việc ngăn chặn các hành động khủng bố". Thay vào đó, như tờ *Washington Post* đã lưu ý, trong hầu hết các trường hợp nơi mà các âm mưu đã bị phá vỡ thì nghiên cứu đã thấy rằng "sự ép tuân thủ luật và các phương pháp điều tra theo truyền thống đã đưa ra đầu mối hoặc bằng chứng để khởi xướng vụ việc".

Hồ sơ đó quả thực hoàn toàn nghèo nàn. Hệ thống thu thập tất cả đã không làm gì để dò tìm ra, để lại một mình phá vỡ, tờ *Boston Marathon* năm 2012 bỏ bom. Nó đã không dò tìm ra ý định của việc ném bom ngày lễ Giáng sinh của một máy bay phản lực bay qua Detroit, hoặc chiếc máy bay đã bay vào Quảng trường Thời đại (Times Square), hoặc âm mưu tấn công hệ thống tàu điện ngầm của Thành phố New York - tất cả chúng đã bị những người ngoài cuộc cảnh báo hoặc các lực lượng cảnh sát truyền thống làm dừng. Nó thực sự đã không làm gì để dừng chuỗi nổ súng giết người hàng loạt từ Aurora tới Newtown. Các cuộc tấn công quốc tế chính từ Luân đôn tới Mumbai tới Madrid đã diễn ra mà không có sự dò tìm ra, bất chấp có liên quan tới ít nhất hàng tá các đặc vụ.

Và bất chấp những tuyên bố khai thác từ NSA, sự giám sát cả đống có thể đã không đưa ra được cho các dịch vụ tình báo các công cụ tốt hơn để ngăn chặn cuộc tấn công ngày 11/09. Keith Alexander, nói trước ủy ban tình báo Hạ viện, đã nêu: "Tôi thà ở đây hôm nay tranh luận" về chương trình đó "còn hơn cố giải thích cách mà chúng tôi đã thất bại để ngăn chặn một ngày 11/09 khác". (Lý lẽ tương tự, đúng nguyên văn, đã xuất hiện trong việc nói lên những điểm mà NSA đã trao cho các nhân viên của mình để sử dụng để chống đỡ các câu hỏi).

Ngụ ý là việc reo rắc nỗi sợ hãi có hạng và gian dối cùng cực. Như nhà phân tích về an ninh của CNN Peter Bergen đã chỉ ra, CIA đã nhân các báo cáo về một âm mưu của Al-Qaeda và "khá nhiều thông tin về 2 kẻ chuyên đánh chặn và sự hiện diện của chúng ở nước Mỹ", mà "cơ quan đó đã không chia sẻ với các cơ quan khác của chính phủ cho tới khi nó đã quá muộn để làm bất kỳ điều gì về nó".

Lawrence Wright, chuyên gia về Al-Qaeda của tờ *New York Times*, cũng đã bóc trần tuyên bố của NSA rằng thu thập siêu dữ liệu có thể làm dừng vụ 11/09, giải thích rằng CIA "đã từ chối tình báo cốt yếu từ FBI, nơi có quyền cuối cùng để điều tra chủ nghĩa khủng bố ở nước Mỹ và các cuộc tấn công vào những người Mỹ ở nước ngoài". FBI có thể đã dừng được vụ ngày 11/09, ông đã viện lý.

> Nó đã có một lệnh cho phép thiết lập sự giám sát bất kỳ ai có liên hệ với Al Qaeda ở nước Mỹ. Nó có thể đi theo họ, áp vào các điện thoại của họ, sao chép máy tính của họ, đọc các thư điện tử của họ, và thu thập các hồ sơ y tế, ngân hàng và thẻ tín dụng của họ. Nó đã có quyền yêu cầu các hồ sơ từ các công ty điện thoại của bất kỳ cuộc gọi nào mà họ đã thực hiện. Đã không có nhu cầu đối với một chương trình thu thập siêu dữ liệu. Những điều từng cần thiết là sự cộng tác với các cơ quan liên bang khác, nhưng vì lý do cả lặt vặt và tù mù

> mà các cơ quan đó chọn ẩn dấu các manh mối sống còn đối với các nhà điều tra có khả năng nhất để ngăn chặn các cuộc tấn công.

Chính phủ từng sở hữu tình báo cần thiết nhưng đã thất bại để hiểu hoặc hành động về nó. Giải pháp là nó sau đó bắt tay vào - để thu thập mọi thứ, một cách ồ ạt - đã không làm gì để sửa sự thất bại đó.

Hơn nữa và hơn nữa, từ nhiều góc cạnh, sự viện dẫn về mối đe dọa của chủ nghĩa khủng bố đã được mở ra như một sự giả vờ.

Trong thực tế, sự giám sát ồ ạt đã có hiệu ứng hoàn toàn ngược lại: nó làm cho việc dò tìm và dừng khủng bố khó khăn hơn. Nghị sỹ quốc hội đảng Dân chủ Rush Holt, một nhà vật lý và là một trong số ít các nhà khoa học trong Quốc hội, đã đưa ra một điểm rằng việc thu thập mọi thứ về các giao tiếp truyền thông của từng người chỉ làm mờ đi các âm mưu thực sự khi được các tên khủng bố thực sự thảo luận tới. Được định hướng hơn là giám sát bừa bãi có thể có được thông tin đặc thù và hữu dụng hơn. Tiếp cận hiện hành làm mất tác dụng các cơ quan tình báo với quá nhiều dữ liệu mà họ không thể có khả năng phân loại nó một cách có hiệu quả.

Ngoài việc cung cấp quá nhiều thông tin, các sơ đồ giám sát của NSA kết thúc bằng việc làm gia tăng chỗ bị tổn thương của đất nước: các nỗ lực của cơ quan đó để vượt qua các phương pháp mã hóa bảo vệ cho các giao dịch Internet phổ biến - như ngân hàng, các hồ sơ y tế, và thương mại - đã để lại cho các hệ thống đó bị mở ra cho sự thâm nhập của các tin tặc và các thực thể thù địch khác.

Chuyên gia an ninh Bruce Schneier, viết trên *Atlantic* vào tháng 01/2014, đã chỉ ra:

> Giám sát ở khắp mọi nơi không chỉ là không hiệu quả, mà nó còn là cực kỳ tốn kém... Nó phá vỡ các hệ thống kỹ thuật của chúng ta, khi các giao thức cơ bản của Internet đã trở nên không được tin cậy... Đây không phải là sự lạm dụng chỉ trong nội địa mà chúng ta phải lo lắng; mà cả phần còn lại của thế giới nữa. Chúng ta càng chọn nghe lén Internet và các công nghệ giao tiếp truyền thông khác bao nhiêu, thì chúng ta càng ít có an ninh từ việc nghe lén từ những người khác. Sự lựa chọn của chúng ta không phải giữa một thế giới số nơi mà NSA có thể nghe lén và một thế giới nơi mà NSA ngăn chặn được khỏi việc nghe lén; đó là giữa một thế giới số mà bị tổn thương đối với tất cả những kẻ tấn công, và một thế giới mà là an ninh cho tất cả những người sử dụng.

Những gì có lẽ là đáng lưu ý nhất về sự khai thác vô đáy mối đe dọa của chủ nghĩa khủng bố là việc nó bị thổi phồng quá đáng. Rủi ro của bất kỳ cái chết nào của người Mỹ trong một cuộc tấn công khủng bố cũng là nhỏ vô cùng, ít hơn đáng kể so với cơ hội bị sét đánh. John Mueller, một giáo sư của Đại học Bang Ohio, người đã viết nhiều về sự cân bằng giữa mối đe dọa và các chi tiêu trong việc chống chủ nghĩa khủng bố, được giải thích trong năm 2011: "Số những người trên thế giới mà bị các tên khủng bố dạng đạo Hồi, những kẻ đóng thế của Al Qaeda giết chết, có lẽ là vài trăm người bên ngoài các vùng chiến sự. Về cơ bản số người y hệt bị chết đuối trong bồn tắm mỗi năm".

Nhiều công dân Mỹ hơn đã chết "không bị hoài nghi" "ở nước ngoài từ các tai nạn giao thông hoặc các bệnh đường ruột", McClatchy của cơ quan tin tức đã nêu, "hơn là từ chủ nghĩa khủng bố".

Ý tưởng rằng chúng ta sẽ triệt phá các bảo vệ cốt lõi của hệ thống chính trị của chúng ta để xây dựng một nhà nước giám sát ở khắp mọi nơi vì lợi ích của nguy cơ này là bất hợp lý cao độ. Vâng sự thổi phồng mối đe dọa được lặp đi lặp lại hết lần này tới lần khác. Ngay trước thềm Olympics 2012 ở Luân Đôn, sự tranh cãi đã bùng phát được cho là về một sự thiếu an ninh. Công ty được ký hợp đồng để cung cấp an ninh đã thất bại để chỉ ra số lượng người canh gác cần thiết theo hợp đồng của mình, và hét toáng lên từ khắp mọi nơi trên thế giới khăng khăng rằng các môn thể thao vì thế đã bị tổn thương đối với một cuộc tấn công khủng bố.

Sau kỳ Olympics không có sự cố nào, Stephen Walt đã lưu ý trên tờ *Foreign Policy* rằng sự la hét từng được dẫn dắt, như thường lệ, từ sự thổi phồng nghiêm trọng mối đe dọa đó. Ông đã trích dẫn một bài của John Mueller và Mark G. Stewart trong *An ninh Quốc tế* (*International Security*) theo đó các tác giả đã phân tích 50 trường hợp "các âm mưu khủng bố hồi giáo" có ý định chống lại nước Mỹ, thì chỉ kết luận rằng "hầu hết tất cả các thủ phạm từng là 'không có khả năng, không có hiệu quả, không có hiểu biết, ngu xuẩn, thờ ơ, không có tổ chức, không có chỉ dẫn, lộn xộn, không chuyên nghiệp, lơ mơ, không thực tế, khờ dại, không hợp lý, và ngu ngốc'". Mueller và Stewart đã trích từ Glenn Carle, cựu phó quan chức tình báo quốc gia về các mối đe dọa xuyên biên giới, người đã nói: "Chúng ta phải thấy những tên Jihad đối với những người chống đối nhỏ, gây chết người, thất vọng và cùng khổ mà họ là", và họ đã lưu ý rằng "các khả năng của Al-Qaeda là thấp kém hơn nhiều so với mong muốn của nó".

Dù vậy, vấn đề là có quá nhiều phe phái quyền lực với quyền lợi được ban trong nỗi sợ hãi của chủ nghĩa khủng bố: chính phủ, tìm kiếm sự chứng minh cho các hành động của mình; sự giám sát và các nền công nghiệp vũ khí, chìm trong việc cấp vốn nhà nước; và các phe phái quyền lực thường trực ở Washington, đã cam kết thiết lập các ưu tiên của họ mà không có thách thức thực tế. Stephen Walt đã đưa ra điểm mấu chốt này:

> Mueller và Stewart ước tính rằng các chi tiêu trong an ninh nội địa (nghĩa là, không tính tới các cuộc chiến tranh ở Iraq và Afghanistan) đã gia tăng hơn 1 tỷ USD kể từ ngày 11/09, thậm chí dù rủi ro thường niên bị chết trong một cuộc tấn công khủng bố nội địa là khoảng 1 trong 3.5 triệu. Sử dụng các giả thiết bảo thủ và các đánh giá rủi ro theo phương pháp luận truyền thống, thì họ ước tính rằng để các chi tiêu đó trở nên có hiệu quả về chi phí thì "họ có thể đã phải ngăn chặn, ngăn ngừa, đẩy lui hoặc bảo vệ chống lại được 333 cuộc tấn công rất lớn mà có thể nếu không thì chúng đã thành công được mỗi năm". Cuối cùng, họ lo ngại rằng ý thức bị thổi phồng sự nguy hiểm này bây giờ đã bị "nội địa hóa": thậm chí khi các chính trị gia và "các chuyên gia khủng bố" sẽ không thổi phồng sự nguy hiểm, thì công chúng vẫn thấy mối đe dọa đó là lớn và nổi bật.

Khi nỗi sợ hãi khủng bố từng bị điều khiển, thì sự nguy hiểm được chứng minh về việc cho phép nhà nước vận hành một hệ thống giám sát bí mật ồ ạt đã bị công bố không đúng sự thật một cách

nghiêm trọng.

Thậm chí nếu mối đe dọa khủng bố từng ở mức như được chính phủ nêu, thì điều đó vẫn có thể không minh chứng được cho các chương trình giám sát của NSA. Các giá trị khác với an ninh vật lý ít nhất dường như không quan trọng hơn. Nhận thức này từng được nhúng vào trong văn hóa chính trị của nước Mỹ từ sự khởi đầu của đất nước này, và sống còn không kém đối với các nước khác.

Các quốc gia và các cá nhân thường xuyên tiến hành các lựa chọn đặt các giá trị của tính riêng tư và, một cách âm thầm, quyền tự do lên trên các mục tiêu khác, như an ninh vật lý. Quả thực, mục tiêu cốt lõi của Sửa đổi bổ sung số 4 trong Hiến pháp Mỹ là để cấm các hành động cảnh sát như vậy, thậm chí dù chúng có thể làm giảm tội phạm. Nếu cảnh sát có khả năng đột nhập vào bất kỳ ngôi nhà nào mà không cần lệnh cho phép, thì bọn giết người, bọn phạm tội hiếp dâm, và bọn bắt cóc có thể dễ dàng bị bắt được hơn. Nếu nhà nước được phép đặt các bộ giám sát trong các ngôi nhà của chúng ta, thì tội phạm có thể giảm đáng kể (điều này chắc chắn đúng đối với bọn trộm cắp trong nhà, vâng hầu hết mọi người có thể giật nảy với phép chữa trị trước triển vọng đó). Nếu FBI được phép nghe các cuộc hội thoại của chúng ta và tóm lấy các giao tiếp truyền thông của chúng ta, thì một dải rộng lớn các tội phạm có thể hình dung được sẽ bị ngăn chặn và giải quyết.

Nhưng Hiến pháp từng được viết để ngăn chặn những xâm lấn không có nghi ngờ gì như vậy đối với nhà nước. Bằng việc vẽ ra một đường trong các hành động như vậy, chúng ta biết cho phép khả năng có thể xảy ra sự phạm tội còn lớn hơn. Vâng chúng ta đã vẽ ra đường đó rồi, thể hiện cho bản thân chúng ta mức độ nguy hiểm cao hơn, vì việc theo đuổi an toàn vật lý tuyệt đối chưa bao giờ từng là ưu tiên xã hội bao quát toàn bộ duy nhất của chúng ta.

Thậm chí trên cả sự thịnh vượng vật lý của chúng ta, một giá trị trung tâm là giữ cho nhà nước tách khỏi lãnh địa của tư nhân - "những con người, các ngôi nhà, các giấy tờ và các hiệu quả" của chúng ta như Sửa đổi bổ sung số 4 đã đặt ra. Chúng ta làm thế chính xác vì lãnh địa đó là sự thử thách tôi luyện của quá nhiều thuộc tính điển hình có liên quan tới chất lượng cuộc sống - tính sáng tạo, sự khai phá, sự thân mật.

Việc từ bỏ tính riêng tư trong cuộc tìm kiếm sự an toàn tuyệt đối là có hại cho một tinh thần và cuộc sống lành mạnh của một cá nhân vì nó là để phục vụ cho một nền văn hóa chính trị lành mạnh. Đối với cá nhân, an toàn trước hết có nghĩa là một cuộc sống tê liệt và sợ hãi, không bao giờ bước vào một chiếc ô tô hoặc máy bay, không bao giờ tham gia trong một hoạt động kéo theo sự rủi ro, không bao giờ cân nhắc chất lượng cuộc sống hơn số lượng, và trả bất kỳ giá nào để tránh sự nguy hiểm.

Việc reo rắc nỗi sợ hãi là một chiến thuật được ưa chuộng của các nhà chức trách chính xác vì nỗi sợ hãi quá có sức thuyết phục để hợp lý hóa sự bành trướng quyền lực và cắt xén các quyền. Ngay từ đầu của cuộc chiến chống khủng bố, những người Mỹ thường xuyên được nói rằng họ phải từ bỏ các quyền chính trị cốt lõi của họ nếu họ sẽ phải có bất kỳ hy vọng nào tránh thảm họa. Từ chủ tịch Tình báo Thượng viện Pat Robert, ví dụ: "Tôi là người ủng hộ mạnh mẽ Sửa đổi bổ sung điều 1, Sửa đổi bổ sung điều 4 và các quyền tự do dân sự. Nhưng bạn không có các quyền tự do dân sự nếu bạn chết". Và thượng nghị sỹ GOP John Cornyn, người quản lý tái bầu cử ở Texas với một video về bản thân ông như một cậu bé bất khuất trong một chiếc mũ cao bồi, đã đưa ra một bài tán ca nhút

nhát về lợi ích của việc vứt bỏ các quyền: "Không trong số các quyền dân sự của bạn có ý nghĩa gì nhiều sau khi bạn chết".

Ông chủ của chương trình Nói chuyện (Talk) trên radio Rush Limbaugh bồi thêm, cho hiển thị sự thờ ơ trong lịch sử bằng việc hỏi khán phòng lớn của ông: "Lần cuối là khi nào bạn nghe thấy một tổng thống tuyên bố chiến tranh trên cơ sở rằng chúng ta sẽ đi bảo vệ các quyền dân sự của chúng ta nhỉ? Tôi không thể nghĩ về một lần như thế...

Các quyền tự do dân sự của chúng ta là không có giá trị nếu chúng ta chết! Nếu bạn chết và đặt lên bó hoa cúc, nếu bạn đang hút bụi bên trong cỗ quan tài, bạn có biết các quyền tự do dân sự của bạn có đáng giá không? Ê, bằng 0, này".

Dân chúng, một quốc gia mà tôn thờ an toàn vật lý trên tất cả các giá trị khác cuối cùng sẽ vứt bỏ sự tự do của mình và đồng ý với bất kỳ sức mạnh nào được nhà chức trách chiếm đoạt để đổi lấy lời hứa hẹn, bất kể nó hoang đường tới đâu, về an ninh tổng thể. Tuy nhiên, an toàn tuyệt đối bản thân nó là tưởng tượng không có thật, được theo đuổi nhưng không bao giờ giành được. Sự theo đuổi làm giảm giá trị đối với những ai tham gia vào trong đó cũng như bất kỳ quốc gia nào mà sẽ được nó xác định.

Sự nguy hiểm mà nhà nước vận hành một hệ thống giám sát bí mật ồ ạt đặt ra là điểm xấu hơn nhiều bây giờ so với bất kỳ thời điểm nào trong lịch sử. Trong khi chính phủ, thông qua sự giám sát, biết nhiều hơn và nhiều hơn về những gì các công dân của mình đang làm, các công dân của nó biết ít hơn và ít hơn về những gì chính phủ của họ đang làm, được che chắn như nó là bằng một bức tường bí mật.

Khó để cường điệu cách mà tình huống triệt để tận gốc này đảo ngược được việc xác định động lực của một xã hội lành mạnh hoặc nó dịch chuyển cơ bản thế nào sự cân bằng quyền lực hướng tới nhà nước. Panopticon của Bentham, được thiết kế để ban sức mạnh không thể tranh giành được vào trong tay của các nhà chức trách, từng được dựa vào chính xác sự đảo ngược này: "Bản chất của nó", ông viết, ở lại trong "trung tâm tình trạng của người thanh tra" được kết hợp với "những sáng chế có hiệu quả nhất cho việc giám sát mà không bị nhìn thấy".

Trong một nền dân chủ lành mạnh, điều ngược lại là đúng. Nền dân chủ đòi hỏi trách nhiệm giải trình và sự đồng thuận của cai trị, điều duy nhất có khả năng nếu các công dân biết những gì đang được thực hiện nhân danh họ. Giả thiết là, với ngoại lệ hiếm hoi, họ sẽ biết mọi điều các quan chức chính trị của họ đang làm, điều giải thích vì sao họ được gọi là những người phục vụ công chúng, làm việc trong khu vực nhà nước, trong dịch vụ nhà nước, cho các cơ quan nhà nước. Ngược lại, giả thiết rằng chính phủ, với ngoại lệ hiếm hoi, sẽ không biết điều gì các công dân tuân thủ luật đang làm. Điều đó giải thích vì sao chúng ta được gọi là các cá nhân riêng tư, vận hành trong khả năng riêng tư của chúng ta. Sự minh bạch là dành cho những ai triển khai các nhiệm vụ nhà nước và thực thi quyền lực nhà nước. Tính riêng tư là cho tất cả những người khác nữa.