The New York Review of Books

The Swedish Kings of Cyberwar

Hugh Eakin

JANUARY 19, 2017 ISSUE

On April 24, 2013, just weeks before Edward Snowden went public with his leaks about mass surveillance by the National Security Agency, General Keith B. Alexander, then the head of the NSA, welcomed a group of Swedish intelligence officials to a secret three-day meeting at NSA headquarters in Fort Meade, Maryland. In the delegation were Ingvar Åkesson, the longtime director of Sweden's National Defense Radio Establishment (known as the FRA, for Försvarets radioanstalt), a shadowy Swedish government intelligence agency, and five members of Åkesson's senior staff. One of the aims of the meeting was to discuss Sweden's growing importance to the NSA.

Pete Souza/White House

President Barack Obama with then Swedish Foreign Minister Carl Bildt at Stockholm Arlanda Airport, September 2013. At a joint press conference with then Swedish Prime Minister Fredrik Reinfeldt the same day, Obama discussed surveillance by the NSA.

In a 2008 law, the FRA had been given expansive powers by the Swedish government to vacuum up all communications traveling over fiber optic networks into and out of Sweden—including e-mails, text messages, and telephone calls. This was of great interest to the NSA, not least because a large percentage of Russian communications traveled through Sweden. In 2011, the Swedes began sharing their surveillance data with the nsa, which included—as NSA officials described it at the time of the meeting—a "unique collection [of communications data] on high-priority Russian targets such as leadership, internal politics, and energy."

Noting the Swedish spy agency's unusual technical abilities and reputation for secrecy, NSA officials also viewed it as an ideal collaborator on its hacking and cyberwarfare project, called Quantum. One of the Quantum programs was an ambitious operation called WINTERLIGHT, which aimed at secretly hacking into high-value foreign computers and computer networks to obtain not only communications data but also any information stored on the hard drives or servers in question. Possible targets might be the administrators of foreign computer networks, government ministries, oil, defense, and other major corporations, as well as suspected terrorist groups or other designated individuals. Similar Quantum operations have targeted OPEC headquarters in Vienna, as well as Belgacom, a Belgian telecom company whose clients include the European Commission and the European Parliament.

According to NSA documents, WINTERLIGHT was using a complex attack strategy to secretly implant a malware program on the targeted computer or network. The NSA's malware would then divert any signals between those computers and the Internet through "rogue" high-speed surveillance servers, called "FoxAcid" servers, allowing the NSA to access in stealth almost any of the user's personal data—and even to tamper with data traveling from one user to another. The implications for both spying and offensive cyber operations were far-reaching. *Wired* has described how the attack on the Belgian telecom was able to

> [map] out the digital footprints of chosen workers, identifying the IP [internet protocol] addresses of work and personal computers as well as Skype, Gmail and social networking accounts such as Facebook and LinkedIn. Then they set up rogue pages, hosted on FoxAcid servers, to impersonate, for example, an employee's legitimate LinkedIn

profile page.

Significantly, while WINTERLIGHT was a joint effort between the NSA, the Swedish FRA, and the British GCHQ, the hacking attacks on computers and computer networks seem to have been initiated by the Swedes. The FRA was setting up the implants on targeted computers—known in NSA parlance as "tipping"—to redirect their signals to the surveillance servers, thus allowing the GCHQ and the NSA to access their data, in what are called "shots." At the time of the April 2013 meeting, the NSA reported that "last month, we received a message from our Swedish partner that GCHQ received FRA QUANTUM tips that led to 100 shots."

Since the extraordinary revelations that the Russian government sought to influence the 2016 US presidential election with information hacked from the computers of the Democratic National Committee and top Democratic officials, cybersecurity has become an urgent national priority. As US officials point out, the DNC hacking is only the latest in an accelerating series of Russia-linked cyberattacks aimed at political and other institutions in the West, including the Estonian government and media in 2007, the German Bundestag in 2015, Ukraine's power grid in 2015, and the Swedish media in March 2016. Far less noted, however, has been the extent to which the US itself has coordinated with Sweden and other allies to develop hacking and surveillance tools that are far more advanced than the e-mail "phishing" strategies used in the recent Russian attacks. A major target of this technology is Russia itself.

NSA officials describe their Swedish counterparts as "extremely competent, technically innovative, and trusted," and praised them for being "proficient in collecting a wide variety of communications." Notably, the Swedish FRA had been given access to the NSA's most powerful analytic tool, called XKeyscore, which, according to nsa documents, enables the retrieval from mass surveillance data of "nearly everything a user does on the Internet."

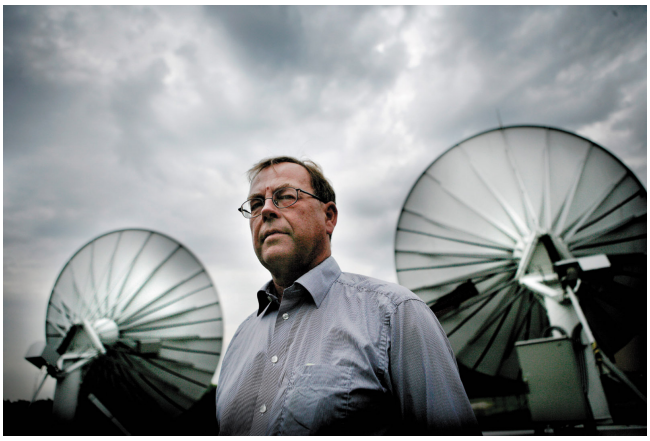
The NSA further noted in its April 2013 report that the FRA "continues to gain access to more data from additional telecommunications companies" and that new Swedish legislation had also given the FRA expanded counterterrorism powers. According to the American agency, the broad leeway given to the FRA had made Sweden a more reliable surveillance ally than Great Britain. One document about the NSA's WINTERLIGHT program reports that "continued GCHQ involvement may be in jeopardy due to British legal/policy restrictions, and in fact NSA's goal all along has been…a bilat[eral arrangement] with the Swedish partner."

In early June 2013, less than six weeks after the Swedish delegation visited Fort Meade, the first reports on NSA spying based on the Edward Snowden leaks were published in *The Guardian* and *The Washington Post*. Over the following weeks and months, Snowden's revelations about the NSA's global surveillance efforts, and in particular its bulk data collection program, called PRISM, set off a protracted debate in the United States and ultimately prompted Congress to implement new restrictions on the NSA in 2015. Similar scrutiny was brought to bear on Britain's GCHQ and its own program called TEMPORA, which aimed to tap directly into transatlantic fiber optic cables to intercept what *The Guardian* described as "vast quantities of global email messages, Facebook posts, internet histories and calls," which it was sharing with the NSA. But the controversy mostly ended there.

In the account that emerged in the British and American press, the NSA and GCHQ programs were generally portrayed as dangerous aberrations—cases of vast intelligence overreach by the two most powerful governments in the Western alliance. To the extent that continental European governments were mentioned, it was as victims of British and American spying: the targets of one or the other had included France's presidential palace and, most notoriously, the cell phone of German Chancellor Angela Merkel. But what if some European governments were themselves pursuing bulk data collection on private citizens, using the exact same methods—and perhaps with even less oversight?

While much remains unclear about the Swedish program, the FRA's status as one of the NSA's most valued foreign partners raises large questions about whether the American and British efforts were so unusual. Though it has been hardly mentioned

in the international press, Sweden's advanced Internet spying apparatus has been noted by Snowden himself. In videotaped testimony to the European Parliament in March 2014, Snowden said, "As it pertains to the issue of mass surveillance, the difference between…the NSA and [the Swedish] FRA is not one of technology, but rather funding and manpower." (The FRA currently has a budget of around $100 million and some 700 employees; the nsa is believed to have a budget of around $10 billion and more than 30,000 employees.)



Magnus Wennman/IBL/REX/Shutterstock

Ingvar Åkesson, director of Sweden's National Defense Radio Establishment (FRA) from 2003 to 2013. In April 2013, he participated in a secret three-day meeting with then NSA Director Keith Alexander in Fort Meade, Maryland, to discuss Sweden's growing importance to the NSA.

Swedish officials have not made any public statements about the WINTERLIGHT hacking program, but in July 2013, when Germany and France pressed the EU to hold talks with US officials to learn more about NSA spying in Europe, Sweden joined the UK in vetoing the move, claiming that the EU had no authority to discuss matters of national security and intelligence.

More recently, the current Swedish government, led by the center-left Social Democrats, has acknowledged that Sweden is pursuing "offensive" cyberwarfare capabilities—which would include hacking—as well as technology to defend against cyberattacks. "The Snowden documents confirmed that there is a very intense cooperation between Sweden and the US," Mark Klamberg, a Swedish legal scholar who has written about the FRA law, told me. "At the top you have the NSA, and below that the GCHQ, and below that you have…Sweden."

In fact, Sweden has been at the vanguard of a rapid expansion of state surveillance across northern Europe. Since Snowden's testimony, Europe has experienced multiple terrorist attacks, the recruitment of thousands of its citizens as foreign fighters in Syria, and a broadening backlash against immigrants and asylum seekers. In recent months, countries ranging from France and Germany to the Netherlands, Austria, Denmark, Finland, and Norway have considered or passed legislation aimed at enabling greater monitoring of their populations.

On November 17, the British Parliament passed the Investigatory Powers Act, making legal a wide variety of hacking and spying activities by the UK government; *The Guardian* has described it as mandating "the most sweeping surveillance powers in the western world." And with the incoming administration of Donald Trump talking about a large-scale expansion of national security programs in the United States, including a possible return to bulk phone data collection by the NSA—allegedly abandoned in the NSA reform law of 2015—the advanced Western democracies may be entering a new age of secret government snooping.

In many respects, Sweden seems an unlikely country to lead this charge. Widely considered a model social democracy, the Swedish state is known for its advocacy of human rights, its broad protections of social freedoms, its government by consensus, and its expansive welfare state. In contrast to the United States and the UK, national security has never been an overriding concern: Sweden has followed a policy of official neutrality for more than two hundred years, it does not belong to NATO, and it has had only a marginal part in the "war on terror." For much of the past decade, the Swedish government has also been a leading promoter of Internet freedom in the developing world, which it argues is a core element of democracy.

With the rise of the Internet, however, the FRA—a spy agency devoted to radio, radar, and other "signals intelligence"—was in danger of obsolescence. In the early 2000s, it began developing technology to tap into the undersea fiber optic cables on

which nearly all intercontinental e-mails, phone calls, and other communications now travel, and in 2007 and 2008 the Swedish government, then led by the center-right Moderate Party, proposed the law giving the FRA broad access to cable traffic. The spy agency would also be able to store the metadata it extracted—reportedly on a huge database called Titan—for a year. At the time, there were public protests on the steps of parliament and groups like the US-based Electronic Frontier Foundation suggested that such far-reaching surveillance powers would be unprecedented. But in June 2008, after the government made some concessions, including the establishment of a secret oversight court, the law narrowly passed and the debate largely ended.

Five years later, when a Swedish broadcaster revealed the Snowden documents showing Sweden's extensive collaboration with the NSA to spy on Internet users—and even hack into their computers—the response was muted. Unlike in the US, no parliamentary hearings were held. According to Klamberg, the Swedish legal scholar, members of parliament remain in the dark about many aspects of the FRA program and there still may be lack of awareness of its scale. "When the legislation was adopted," he said,

> the message was that it was well regulated and that only small amounts of data would be stored. But when I study the law and read the reports of the Swedish Data Inspection Board, the opposite picture emerges: the surveillance and storage of data is massive, especially when it comes to metadata.

For the NSA and the GCHQ, other analysts suggest, the FRA law has provided a cover for surveillance programs of questionable legality. On December 21, the European Court of Justice sided with challengers to sweeping laws in Sweden and the UK requiring telecom companies to store call and text records, finding that "EU law precludes national legislation that prescribes general and indiscriminate retention of data." Observers have noted similarities between the vaguely worded FRA law and a US law known as the FISA Amendments Act, which also passed in 2008 and which the NSA has cited as the legal basis for its own PRISM program. The Swedish government has also been adept at avoiding scrutiny of its surveillance-sharing with the United States, perhaps by keeping some of those arrangements informal. (According to a diplomatic cable published by WikiLeaks, when a US delegation visited Sweden in November 2008 seeking to conclude an intelligence-sharing agreement, officials from the Swedish Justice Ministry demurred, arguing that "existing informal channels, which cover a wide range of law enforcement and anti-terrorism cooperation, would be scrutinized more intensely by Parliament and perhaps jeopardized.")

Nor was Sweden the only Scandinavian country to have embraced mass surveillance in the years before the Snowden revelations. Several NSA documents also mention the Norwegian Intelligence Service (NIS), and in December 2013, the Norwegian newspaper *Dagbladet*, working with the American journalist Glenn Greenwald, reported that Norway was providing the NSA with tens of millions of communications every month. Drawing on NSA documents and sources in Norway, the newspaper revealed that the NIS was targeting Russia in particular, "conducting surveillance against politicians" as well as Russian military and energy targets. It also noted that, with NSA help, the NIS was acquiring a hundred-million-dollar "Windsor Blue derivative supercomputer," called STEELWINTER, to analyze encrypted surveillance data, and that the nis was working with the NSA's cryptanalysis division to do so.

Like Sweden, Norway is often viewed as a successful social democracy with a long record of advocacy for human rights. Norway in particular is known for its robust protections of free speech and its tradition of government transparency. Like Sweden, it has long ranked near the top among Western nations in measures of citizens' trust in government institutions. And while Norway is a member of NATO, it too has stayed mostly on the periphery of the war on terror. Yet Norwegians have been largely unperturbed by revelations about their government's secret collaboration with the NSA.

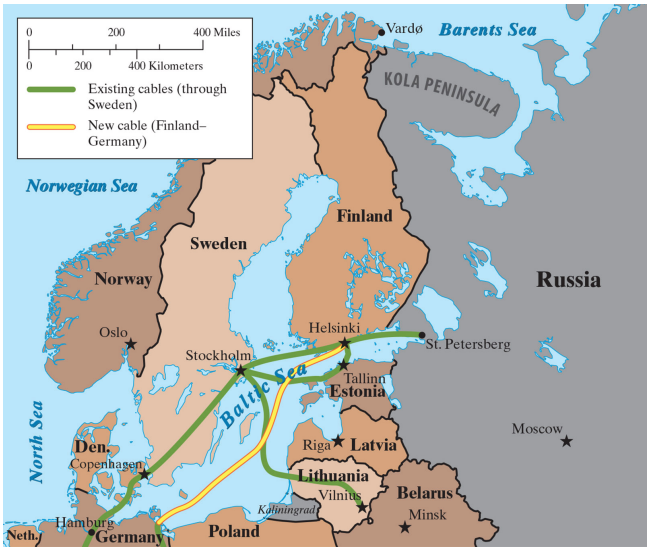
After *Dagbladet*'s report on Norway's bulk surveillance program, there was a brief controversy in the press. But the head of Norwegian intelligence asserted that the data Norway was collecting was from foreign rather than domestic communications and the controversy quickly ended. In Oslo, Karsten Friis, a senior adviser at the Norwegian Institute of International Affairs,

told me that many Norwegians are proud that their country has become so important in American intelligence efforts. "There was the sense that we have this capacity and we're not afraid of talking about it," Friis said. In an article in *Dagbladet*, Greenwald disputed the Norwegian spy chief's claim, arguing that NSA documents show that the data likely includes communications by Norwegians themselves.

By contrast, Norwegians are uneasy about spying by the FRA, because about 80 percent of Norwegian Internet traffic—even domestic communications from one Norwegian to another—travels through Sweden. Partly as a result, the Norwegian parliament has begun debate on a so-called Digital Border Defenses bill, which would, in effect, give Norwegian intelligence similar access to international fiber optic cables as the FRA has.

In October, Bjørn Erik Thon, the head of the Norwegian Data Protection Authority, a government agency responsible for privacy issues, told me that he had serious reservations about the bill, because it would be very difficult to prevent Norwegians' data from being swept up too, despite plans to "filter out" streams of data coming from Norway's own sources. He said that his agency was working on a report critical of the bill. But Thon added that the proposed legislation has met with little resistance among the main parties or in the press and is likely to pass in the coming months. "It's just not a big concern here."

Secret government eavesdropping has a long history in Scandinavia. By virtue of its position on Europe's northern flank with Russia and the east, the Scandinavian Peninsula was crucial to Western intelligence officials during the cold war, and both Norway and Sweden developed sophisticated signals intelligence programs. According to NSA documents, the US agency has had close ties to Norwegian intelligence as far back as the 1950s. With Norway's position as NATO's northern bridgehead against the East, the relationship continued until the Gorbachev period. A Norwegian newspaper recently described a listening post in Vardø, in the far north of the country along Norway's border with Russia, as a "giant ear to the east."



But the NSA's relationship with Sweden may be the most interesting. Though officially neutral, Sweden in fact built very close ties to both NATO and the US security establishment in the late 1940s and early 1950s and was deeply involved in cold war spying operations. Among the intelligence agencies, the Swedes were noted for their technical prowess. According to the Norwegian journalist and intelligence historian Alf Jacobsen, in the 1970s and 1980s, the FRA used the Swedish embassy in Helsinki to intercept Soviet military and diplomatic communications, using equipment provided by the NSA; and working for the CIA, the Swedes successfully broke the diplomatic codes of numerous countries, including Brazil, Zaire, China, Iran, Turkey, Japan, and Czechoslovakia.[1]

In recent years, geographical proximity to Russia and the development of the Internet have provided new reasons for Sweden to maintain its technical edge: there are very few undersea fiber optic cables connecting Russia to the outside world—just six, according to the cable-monitoring organization TeleGeography, out of more than three hundred around the world—and the principal ones pass under the Baltic Sea. In July 2008, when Sweden passed its surveillance law, a diplomatic cable from the US embassy in Stockholm, later published by WikiLeaks, noted that, since "80 percent of Russia's foreign cable-based communications flow through Sweden, the law legalizes Sweden's monitoring of the majority of Russia's trans-border communications."

With the Russian military posing increasing threats against NATO allies since the war in Ukraine, such spying has become even more important. Much as during the cold war, there are frequent reports in the Swedish press about Russian submarine and military activity in the region, and growing calls for a tightened military alliance with NATO and the United States. (In 2015, Sweden joined NATO's Cyber Defense Center, a research and training facility in Tallinn, Estonia, and in June 2016, Sweden signed a new "statement of intent" with the Pentagon, aimed at tightening a defense alliance.)

However, the recent completion of a Finnish undersea cable system called Sea Lion, which routes Internet traffic from Finland directly to Germany, may allow many Russian communications to bypass Sweden. This fall, the Finnish government began discussing surveillance legislation of its own, aimed in part at gaining access to the new cable data. Some Western security analysts now view the Baltic Sea as a main theater in a new cyberwarfare arms race. In October 2015, *The New York Times* reported that

> Russian submarines and spy ships are aggressively operating near the vital undersea cables that carry almost all global Internet communications, raising concerns among some American military and intelligence officials that the Russians might be planning to attack those lines in times of tension or conflict.

Among the many questions posed by Scandinavia's embrace of mass surveillance is one that has lingered at the margins throughout the Snowden debate: Are advanced democracies any different than their authoritarian counterparts in seeking to gain broad access into the private lives of citizens? In a fascinating new study, the Swedish scholars Johan Eriksson and Johan Lagerkvist compared the recent cybersecurity efforts of Sweden and China.[2] On the surface, as they note, the countries could not be more different: the Chinese government regulates its citizens' access to the Internet through a vast "firewall" and system of censorship; Sweden has promoted Internet freedom—the idea that unfettered access to the Internet can help mobilize citizens in developing countries and publicize human rights abuses—around the world. Yet when access to the Internet is set aside, the authors observe, there is very little difference between the two:

> Although Sweden is a liberal democracy and China is an authoritarian one-party state, both states have advanced cyber-surveillance systems and recently for the first time acknowledged offensive cyber-warfare capabilities.

Eriksson and Lagerkvist find it "somewhat puzzling" that mass data collection and communications monitoring have not become a major issue in election campaigns in Western countries—despite, they say, "legal and moral problems related to citizens' integrity and privacy, and the non-transparent nature of government surveillance." Such programs have often put Western leaders in a contradictory spot. One of the most outspoken advocates of Internet freedom, for example, is former Swedish foreign minister Carl Bildt. But Bildt is also a leading defender of Sweden's 2008 surveillance law, which his government pushed through. When Bildt was asked at a forum on Internet freedom in 2013 how he reconciled these two views, he explained that Sweden was doing surveillance for a good purpose. "There is a difference between good states and somewhat less good states," he said.

In fact, the very qualities that have made Sweden and Norway successful models of advanced democracy may also have made their populations more susceptible to government spying. In Norway, the government committee that put forward the mass surveillance legislation now before parliament has argued that such measures "can be justified as necessary in a democratic society." And as Swedish and Norwegian scholars point out, Scandinavian citizens are inclined to assume that if the government says it needs certain powers, then it probably does.

In Oslo, Eirik Lokke, a researcher for a liberal Norwegian think tank who has just written a book about privacy in the digital age, told me that Norwegians are far more concerned about the powers of Google and Facebook to gather information about private citizens than about their intelligence service's spying for the NSA. Such a position, he observed, might be the opposite of the United States, where consumers routinely volunteer much of their private identities to Internet companies, while viewing government surveillance with great skepticism.[3]

Still it is far from clear whether the US efforts to rein in the NSA will be sustained, following the explosive revelations about Russian hacking and the election. Even before the CIA's conclusions were reported in the press, and notwithstanding Trump's own refusal to acknowledge the Russian attack, there were indications that the incoming administration would favor a dramatic expansion of surveillance powers. In late November, noting that two Trump appointees in law enforcement and intelligence, Jeff Sessions as attorney general and Mike Pompeo as director of the CIA, are "leading advocates for domestic government spying," *Bloomberg News* reported:

> In a reversal of curbs imposed after Edward Snowden's revelations in 2013 about mass data-gathering by the NSA, Trump and Congress may move to reinstate the collection of bulk telephone records, renew powers to collect the content of e-mails and other internet activity, ease restrictions on hacking into computers and let the FBI keep preliminary investigations open longer.

While continuing to erode our privacy, it is doubtful how much these steps would enhance national security. Chris Soghoian, a privacy and cybersecurity expert for the ACLU, told me, for all the billions of dollars the NSA and its allies have invested in "offensive" cyber technology, the rather crude Russian attacks on the DNC showed the extent to which we have failed to implement basic precautions against cyberattacks at home. Among the many paradoxes of the recent US presidential election, one must surely be that a wave of anti-establishment, populist anger has brought to power a government that stands poised to embark on what could be the greatest expansion of secret state surveillance since the September 11 attacks. If it does so, it may find itself in concert with some of the most open and advanced democracies in Europe.

—December 22, 2016

---

1 Alf R. Jacobsen, "Scandinavia, Sigint and the Cold War," in *Secrets of Signals Intelligence During the Cold War and Beyond*, edited by Matthew M. Aid and Cees Wiebes (Routledge, 2001). ↩

2 Johan Eriksson and Johan Lagerkvist, "Cyber Security in Sweden and China: Going on the Attack?," in *Conflict in Cyberspace*, edited by Karsten Friis and Jens Ringsmose (Routledge, 2016). ↩

3 See Sue Halpern's recent article "They Have, Right Now, Another You," *The New York Review*, December 22, 2016. ↩