Potential Cyber Warfare Capabilities of Major Technology Vendors

Audun Jøsang
University of Oslo, Norway
josang@ifi.uio.no

Abstract:
The Snowden revelations of 2013 gave the public an insight into the cyber surveillance capabilities of the NSA. These capabilities depend largely on the collaboration from some of the major providers of online services and from social network providers such as Facebook and Google. A topic that has not received much focus are the potential cyber operations capabilities and advantages that governments could obtain through the collaboration with major domestic technology companies, such as the software vendor Microsoft and hardware vendor Intel in the USA, or the telecommunication network equipment vendor Huawei in China. While the Snowden revelations focused on surveillance capabilities, the potential collaboration with software and hardware vendors could give tremendous offensive cyber operations capabilities. This paper discusses the cyber warfare capabilities that could be gained through the collaboration with major software and hardware vendors as well as with IT service providers, and explores the political conditions for this type of collaboration to take place and the possible consequences of such scenarios.

Keywords: Cyber operations, Industry collaboration, Snowden revelations, Operating system, Hardware.

1. Introduction

The term ‘cyber operations’ is often used to denote the set of methods used for cyber warfare. Surveillance, defense and attack in cyberspace are general elements of cyber operations that in turn can be decomposed into more specific elements.

In its policy document (White House, 2012) the US administration defines cyber operations as consisting of: “Cyber Collection, Defensive Cyber Effects Operations (DCEO) and Offensive Cyber Effects Operations (OCEO)”. To our knowledge the US administration is the only one in the world that officially has a cyber operations policy clearly articulated in this way. Obviously many other national administrations also practice cyber operations, but policy makers in nation states can reason that there is no need to publish their cyber operations policies because these activities are relatively easy to hide from the public. We find laudable the US administration’s publication of their cyber operations policy because it reduces confusion and contributes to transparency in the cyber warfare landscape, which in turn is beneficial for political stability.

According to the same policy document, surveillance through computer networks is called ‘Cyber Collection’ which is defined as: “Operations and related programs or activities conducted [...] for the primary purpose of collecting intelligence - including information that can be used for future operations - from computers, information or communications systems, or networks with the intent to remain undetected. Cyber collection entails accessing a computer, information system, or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access. [...]”

Methods for surveillance of global communication networks are many and diverse, ranging from interception of communication passing through cables or through the air, to obtaining data stored in databases and being processed within computer hosts. Data can often be intercepted without the authorization and collaboration of the network or host owners as described in the cyber collection policy cited above, but surveillance capabilities can be significantly amplified with their collaboration. The revelations from late 2012 and throughout 2013 by Edward Snowden about NSA’s surveillance capabilities clearly documented that the NSA (US National Security Agency) obtained active collaboration from several prominent companies in order to enhance NSA’s surveillance capabilities. This was done e.g. by having arrangements with companies like Apple, Google and Facebook for obtaining access to customers’ data and profiles (Greenwald and MacAskill, 2013), which in fact is legal according to the USA PATRIOT Act (107th US Congress, 2001).

It has also been revealed that NSA paid US$ 10 million to RSA, a major security technology vendor, to include a backdoor in one of their cryptographic products, thereby enabling the NSA to read traffic encrypted with that product (Menn, 2013). This form of surveillance based on active and consenting...
collaboration with private companies can be considered to be a form of authorized access and therefore seems to extend the scope of the above cited cyber collection policy. However, when assuming that the targets of surveillance are the customers of the collaborating parties, not the collaborating companies, then the surveillance falls under the definition of unauthorized ‘cyber collection’ as cited above. In fact, the collaborating companies become part of the surveillance operations targeted at their own customers. In this scenario it is thus meaningful to distinguish between 3 separate parties: 1) the cyber operations agent, 2) the collaborator, and 3) the target of cyber operations.

Defensive and offensive cyber operations can in general be conducted with or without the collaboration of external parties, and similarly to cyber collection, the potential for defensive and offensive cyber operations increases significantly with the assistance of collaborating parties having specific skills or who control specific technologies and ICT infrastructures. In the sections below we explore various methods that potentially could be used for cyber operations and that have not been mentioned in the literature. These methods go far beyond those described through the Snowden revelations.

Collaborating parties in cyber operations can be public or private companies and organizations, or they can be other nation states. In general, the collaborator can be seen as an intermediary between the cyber operations agent and the target. It is normally assumed that there is a friendly relationship between the cyber operations agent and the collaborating party; otherwise the collaborating party should more precisely be seen as a target of cyber operations. It is thus the nature of the business relationship or the political alliance between the cyber operations agent and an involved party that determines whether the involved party is a collaborator or a target of cyber operations.

Various forms of collaboration are possible, ranging from full voluntary and active participation in the cyber operations, to forced and involuntary participation. Although there is a continuum of types of collaboration we find it meaningful to distinguish between active, passive and forced collaboration that we define as follows.

- **Active collaboration** is when representatives of the collaborating party take voluntary conscious actions in order to assist in cyber operations. This is for example the case when Facebook transmits user profiles to NSA, or gives NSA technical access to the data at their discretion.
- **Passive collaboration** is when representatives of the collaborating party voluntarily and consciously do not exercise their right to take actions that could have hindered cyber operations. This is for example the case when RSA discovers a vulnerability in one of their security products which they know can be exploited by NSA, and they do not attempt remove that vulnerability.
- **Forced collaboration** is when national authorities use pressure or a legal right to force the collaborating party to contribute to cyber operations. Forced collaboration is possible when applicable laws dictate the right to obtain information from collaborating parties. This was for example the case when the U.S. government in 2013 obtained a search warrant demanding that Edward Snowden’s e-mail provider, Lavabit, turn over the private SSL keys that protected all web traffic to the site. Lavabit offered paying customers a secure email service that offered the highest possible level of privacy. When faced with the search warrant, Lavabit decided to stop operations rather than betray its own customers (Poussie, 2013).

The form in which collaboration is practiced in cyber operations can have implications for legal liability, ethical standing and public relations of the collaborating party. A company that grants a cyber-operations agent access to its resources could be the target of legal action, public criticism and could suffer damage to its reputation should this collaboration be publicly known. As an attempt to restore their lost reputation, cyber operations collaborators (e.g. Google, Apple, Facebook) identified by the Snowden revelations have argued for legal changes regarding this form of cyber operations (Roberts and Kiss, 2013). IBM issued a statement saying that it will take steps to challenge any order by the US government to hand over data for surveillance purposes (Weber, 2014), but so far there are no cases where this has happened.

The revelation of massive collaboration between NSA and online social network providers has probably resulted in withdrawal by target groups from these networks precisely because they want to avoid being spied upon. From the perspective of NSA’s cyber operations it is therefore likely that the Snowden revelations have reduced the value of collaboration with these social network providers. Said bluntly, if terrorists used Facebook before the Snowden revelations, most likely they do not use Facebook anymore. The secrecy of specific cyber operations is thus crucial for their effectiveness. Another negative side-effect is of course the lost business suffered by the collaborating companies. They would probably have a credible legal
argument for financial compensation of damage to their reputation and resulting losses due to their collaboration with NSA, because they can claim that it unfairly damages their business.

Cyber operations (DCEO, ODEO and Cyber Collection) can in general be exercised with or without the collaboration of external parties. Cyber operations exercised without any collaborating parties will resemble typical cyber attacks that require the exploitation of vulnerabilities in systems and networks, or the manipulation of individuals through social engineering. Exploited and discovered vulnerabilities are constantly being removed or reduced by system vendors and owners. In order to maintain cyber operations capabilities, there is thus a need for continuously developing new attack methods and discovering new vulnerabilities. New and unknown vulnerabilities are constantly being introduced through technology innovation and product development, where most vulnerabilities are introduced by accident through poor security design, but some can be introduced on purpose e.g. as part of cyber operations.

Although old vulnerabilities get fixed, the rate of eradication is eclipsed by the rate of introduction of new vulnerabilities. Numerous players invest considerable resources in trying to discover these vulnerabilities, either to be used in own cyber operations or to be sold and used for profit. For the latter purpose there are unregulated markets for trading security vulnerabilities and zero-day exploits, (Ablon, Libicki, and Golay, 2014). In theory a national cyber operations player could obtain the needed exploits from such markets. However, these markets represent relatively unreliable sources of exploits because the buyer can never be 100% certain that the seller does not offer the same vulnerability to the buyer’s opponents. National states with an offensive cyber operations program therefore need s to also have the necessary capabilities and resources for ‘vulnerability mining’ based on using massive computational resources and analytical methods such as fuzzing which is a form of brute force vulnerability discovery (Sutton, Greene and Amini, 2007). Software vendors, criminals and governments alike engage in fuzzing. Software vendors do it to remove software bugs in their products; criminals do it to develop exploits that can generate profit, and governments do it to sustain their cyber operations capabilities.

2. Potential Cyber Operations Capabilities through Collaboration with Technology Vendors

NSA’s collaboration arrangement with Google, Facebook and other social network providers is mainly used for surveillance purposes. It is interesting to think further and reflect on the cyber operations capabilities that can be obtained with the collaboration from technology vendors such as Microsoft, Apple, Intel and AMD, Dell and HP. These US companies sell products with dominant global market shares, so that they could be harnessed as potent cyberwarfare tools for the US government. Similarly, telecommunication network equipment produced by Huawei and ZTE could potentially be used by the Chinese government in their cyber operations. This possibility has led some governments to ban their products in specific market segments considered part of their national CII (Critical Information Infrastructure), e.g. in Australia (McDuling, 2012) and in the USA (Rogers and Ruppersberger, 2012). The fact that some Western governments have excluded Chinese manufacturer Huawei from critical market segments shows that governments actually consider cyber operations collaboration with technology vendors as a realistic scenario.

Reduced competition with resulting increased costs is an unavoidable negative side-effect of excluding major vendors from offering components when building critical ICT infrastructures. In some Western countries such as Norway where there also has been a debate about the risks of using Huawei components in critical national telecommunication networks, the argument about increased costs was one reason for not excluding Huawei.

The sections below explore various cyber operations methods that potentially can be harnessed with the collaboration of technology providers in the respective domains of 1) OS (Operating Systems), 2) CPU (Central Processing Unit) hardware, 3) computer systems, and 4) Internet clouds.

2.1 Collaboration with Operating System Vendors

Microsoft and Apple develop operating system software for the PC and Mac respectively. Linux OS distributions are developed by multiple vendors, where the code is often open-source. Automated online software update and patching is an integral part and an important feature of these operating systems, which contributes to their security and robustness. Operating systems are large complex software products that therefore necessarily contain high numbers of bugs and vulnerabilities. As soon as a vulnerability has been discovered it can be exploited by people knowing about it. Exploits for known vulnerabilities are being implemented in automated tools which makes exploitation of those vulnerabilities relatively easy even for non-experts. Without the ability to continuously fix such problems operating systems would be hopelessly unreliable and vulnerable to attacks.
The mechanism for updating and patching is based on programming the client operating system to connect to a specific server owned by the vendor on a regular basis, e.g. daily or weekly. The server checks the current status of the software, and triggers the downloading of missing updates and patches to the client operating system. The updating process is totally controlled by the vendor of the operating system and is mostly transparent to the user. The same updating process can be used to make arbitrary changes to the operating system, so the operating system is in practice totally controlled by the vendor. The vendor of a particular operating system can thus install any application on any computer running its operating system. Given that the Windows OS is installed on approximately 90% of all desktop and laptop computers worldwide, the possibility of total control of the majority of client computers worldwide by Microsoft is real. The potential for cyber operations with Microsoft as collaborating party is thus massive. The possibilities range from cyber collection as in surveillance to offensive cyber effects operations as when actively controlling individual computers like a bot machine.

It is unknown to the public whether operating system vendors like Microsoft collaborate with NSA for surveillance and control of individual computers. While the extent of surveillance through Google, Facebook and Apple was shocking to many, collaboration with e.g. Microsoft for controlling individual computers or clusters of computers would have been even more disturbing to the public. There is thus a significant risk for an OS vendor to collaborate in cyber operations. In the case of Microsoft with almost monopolistic market dominance, the consequence of revealing cyber operations collaboration to the public would be hard to predict. On the one hand, cyber operations victims would be reluctant to continue using Windows, but on the other hand there would in many cases be no real alternative. However severe the negative market consequences of cyber collaboration with OS vendors, if a government perceives the threat of e.g. a catastrophic terrorist attack to be sufficiently high, and the only way to uncover or stop the plot is e.g. through controlling computers through OS update, it would arguably be rational to do precisely that.

2.2 Collaboration with CPU and Microchip Vendors

The layer underneath the OS is typically the CPU hardware. The two main CPU vendors for servers and personal computers are Intel and AMD who share the global market between them and who compete on innovation. Close cooperation between the CPU and operating system vendors leads to rapid innovation and steady increase in performance. This cooperation also results in significant security innovation e.g. to prevent buffer overflow attacks, and to enable secure virtualization of multiple operating systems running simultaneously on the same computer.

It would be possible to implement special triggers that could change the behavior of CPUs as an element of cyber operations to take control of computers. Knowledge of such triggers would enable the control of a computer independently of the operating system running on the computer.

Similar business risks to those mentioned in Sec.2.1 above would exist in case Intel and AMD engage in this form of cyber operations collaboration with NSA. These companies could suffer severe loss of trust from the market should this form of collaboration be revealed, but since they have a monopolistic position it would be difficult for targets to switch to alternative vendors.

Trusted computing is the term used when security functions are based on specialized security hardware. The TPM (Trusted Computing Platform) is a specialized security chip that is integrated on the motherboard of most modern computers shipped today. The role of the TPM is mainly to verify the integrity of low level software such as BIOS and kernel. This can e.g. be used to detect malware infection on the computer. The TPM also has the potential of preventing owners from making certain configuration changes to their own computers, because the TPM dictates certain parts of the configuration and can also dictate which BIOS and OS kernel that can be loaded into memory. In case an exploit has been built into the BIOS or kernel of a computer equipped with TPM, then it might be impossible for the owner to remove those exploits.

2.3 Collaboration with System Vendors

During 2013 it was revealed that the NSA disposes of an extensive set of exploits against a large number of IT products (Appelbaum, Horchert and Stöcker, 2013). The exploits are e.g. based on injecting code into the BIOS or kernel of operating systems of computers which can activate network communication, microphone or camera, or it can be tiny hardware chips that can be integrated into systems such as mobile phones, personal computers, servers, routers and firewalls, from major technology vendors such as Dell, HP, Cisco and Apple. It is important to notice that these exploits do not necessarily imply direct collaboration with these technology vendors. It is theoretically possible that the technology vendors have not played any role in developing these exploits, but it is also possible that they assisted in their development, or actually developed the exploits themselves. The revelation of exploits does not say anything about their origin. So even if a vendor
participated in the development of an exploits against its own products, and the exploit, but not its origin, is revealed to the public, then it does not necessarily result in lost trust from the market.

There is a huge logistic challenge when executing an exploit like integrating a specialized hardware chip on the motherboard of a computer for cyber operations purposes. It would require physical access to the computer, preferably before it is shipped to the target party. It has been suggested that it can be done during shipping with the collaboration of postal or courier service operators (Appelbaum, and Horchert, and Stöcker, 2013). It would probably be much simpler when done at the assembly line of companies like Dell or HP, or during customization by the local distributors, but the logistic challenge would be significant even here.

2.4 Collaboration with Cloud Providers

Another domain of government-industry collaboration with great potential for cyber operations could be in the cloud services industry, whereby a cloud service provider grants its national government passive or active access to customer data and processing. Severe negative consequences for the industry player would of course be the result should this form of collaboration become publicly known. Primarily it would have resulted in significant loss of trust and lost business for the collaborating party because targets for cyber operations would switch to alternative cloud providers.

Online social networks can be considered as a form of cloud service, so for surveillance purposes cyber collection collaboration with cloud providers would be very similar. The topic of offensive cyber operations with a cloud provider is difficult to describe or categorize, and because there is a broad range of possibilities the potential is unclear. The potential for exploiting the various cloud service models such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) should be considered separately. Online social networks can be considered as SaaS cloud service. Cyber operations based on exploiting PaaS could e.g. consist of collecting and analyzing customer data, while cyber operations based on exploiting IaaS in addition would give access to entire virtual IT infrastructures of specific targets.

The debate around the security of cloud services is mostly centered on privacy, but national security is probably even more critical. Cloud services are frequently used even though users often do not consider then as such. For example, an online email service such as provided by hotmail.com or gmail.com is an example of SaaS. Nations states and organizations often outsource the operation of their respective DNS servers, which also can be considered to be a form of SaaS. This potentially makes these nations and organisations particularly vulnerable to a broad range of attacks should the DNS cloud service provider take part in cyber operations by other nation states.

3. Discussion and Conclusion

The crucial question is whether the US and other national governments would want to take advantage of, or are already taking advantage of, collaboration with technology vendors for the purpose of conducting cyber operations. A simple mental walk-through of possible scenarios reveals that such collaboration would give considerable advantages in cyber warfare situations. For example, every running Windows operating system connects to a Microsoft server daily to check for software and configuration updates. From a technical perspective this gives Microsoft full control of every computer on the planet, as well as in space, that runs Windows and that is connected to the Internet. It would be relatively simple to identify the computers of individuals, as well as computers of a specific organization or in a specific geographical region. Remote control of each computer could be used e.g. for espionage or for sabotage, the possibilities are endless. The same type of capabilities would be available for major microprocessor vendors Intel or AMD, where hidden hardware functions could allow remote parties to take control of computers, or telecommunication systems vendors such as Huawei or Cisco where backdoors into the systems could provide a cyber operations agent with unlimited access to network traffic. As the Snowden revelations have shown us, private corporations are willing to, or are legally obliged to collaborate with their national government, so the possibility of remote control of computers through collaboration with vendors of operating system software and hardware is realistic.

When major IT industry players become collaborators in cyber operations a natural consequence is that the market share of their products and services will be determined by global political divisions. For example, if it were the case that a US-based vendor implements a back door for the NSA in their products, and this became publicly known, then a likely result is that markets in countries that are mostly US-antagonistic would stop using these products for fear of being subject to control and surveillance.

It will necessarily have consequences when major technology vendors become collaborators in cyber operations, and this fact becomes known, either publicly or in the intelligence communities. The need for independence of nation states and for global political balance will tend to create a more fragmented global
market of IT products and services. We see some of this taking place already, such as when Google during the period between 2010 and 2013 has been pressured out of the Chinese market or when Huawei is being excluded from US and Australian markets. For outsiders without access to the military intelligence communities all we see at the surface are sporadic conflicts between national governments and technology providers. These incidents are probably only the tip of the iceberg in the global politics of ICT and cyber warfare, and reflect a trend towards Balkanisation of technology.

References


