The Militarization of Cyberspace

Implications for the Private Sector

Originally published in the November 2014 ISSA Journal

By Constantinos Macropoulos and Keith M. Martin – ISSA member, UK Chapter

Cyberspace is now viewed by many states across the globe as critical national infrastructure and cybersecurity as essential to successful governance of their nations. Yet the actions of states betray a bias towards an offense-oriented focus on cybersecurity issues, a bias that carries with it significant implications for the private sector and, in particular, the information security professionals who work within it.

Abstract

The past decade has seen a dramatic acceleration of government involvement in cybersecurity. Cyberspace is now viewed by many states across the globe as critical national infrastructure and cybersecurity as essential to successful governance of their nations. Yet the actions of states betray a bias towards an offense-oriented focus on cybersecurity issues, a bias that carries with it significant implications for the private sector and, in particular, the information security professionals who work within it. We suggest that now is an important time for the information security profession to avert its focus on the technical and operational minutiae of the problem, and step back to contemplate the implications of the wider picture.

Over the past decade we have seen a steady militarization of cyberspace, generating heated debate and endless speculation. During this time we have seen governments engage to a much greater degree in cybersecurity. Many governments regard cyberspace as an essential component of their critical national infrastructure. As a result they see cybersecurity as a significant issue that underpins their ability to operate the state and oversee the well-being of their citizens. Inherent in the designation of cyberspace as critical national infrastructure is the inclusion of the national security establishment by policy makers when devising and implementing cybersecurity strategy.

Yet the discovery of Stuxnet and its viral stable mates, advancements in legal thinking on the applicability of international law on cyber warfare, and a flood of revelations relating to global surveillance programs have given us a somewhat troubling glimpse of how state involvement in cybersecurity is manifesting itself. For the information security community at large this poses significant new security challenges and raises serious questions around the future role of information security practitioners, particularly those operating in the private sector.

As information security practitioners, we are adept at identifying potential dangers based on events that are unfold-

ing and linking them to past events already unfolded. This is essentially how we make our living. Arguably our greatest strength is our ability to work amongst the weeds and focus on the details of a given security problem, deconstruct it, and identify a solution. Unfortunately, this is also a potential weakness; with respect to any form of militarization, one needs to step back and take in the bigger picture lest the forest be lost amongst the trees.

The militarization of cyberspace

For over a year now we have been so focused on mass surveillance activities conducted by national intelligence bodies that we have, to an extent, forgotten other types of state-sanctioned cyber activities. Governments, perhaps out of disinterest, ignorance, and fear, have effectively abdicated responsibility for cyberspace to military subordinates. Military actors view cyberspace as a war-fighting domain that is as ungoverned as Somalia and is a budgetary blessing in these straitened economic times. Incidents like Stuxnet have given us only a glimpse of what is possible when the cyber capabilities of intelligence services and armed services work in unison.

At a fundamental level, from the perspective of the state and its subordinates, the main objective within cyberspace is not ubiquitous Internet surveillance; it is to "dominate" cyberspace. This desire for control looks well beyond the confines of the Internet and encompasses air-gapped networks, firewalled corporate networks, and overlay networks and touches every layer of the OSI model from end to end.

Cyberspace has many appealing features for military actors. Foremost, it provides an opportunity to conduct offensive operations, safe in the knowledge that attribution is difficult. Operations can be conducted from the comfort of national borders, yet an attack may appear, at least to cursory examination, to have originated from almost anywhere. And if it is ever traced back, there will always be grounds for plausible deniability. Further, cyber-offensive operations also keep personnel out of harm's way. This is a significant feature of warfare that has begun to dominate the technology and tactics of the Western military establishment.

Cyberspace warfare aspirations are, of course, not limited to Western governments. Many states around the world are accelerating development of their own cyber-offensive capabilities. Indeed the development of an offensive capability in cyberspace offers the potential appeal of relatively low entry costs compared to the development of more traditional infrastructure and weaponry.

Collateral damage

The irony here is that the very states that are pushing the boundaries in cyber offense are also the ones that most rely on cyberspace for conducting their day-to-day business. Further, many of the states that are trying urgently to catch up for fear of being left behind are the very ones that are betting on a secure cyberspace to develop their economies.

As we witness the development of a cyber-offensive arms race, in which some states may act responsibly when it comes to exercising cyber power and others undoubtedly will not, it is worth considering the extent to which the private sector is becoming "collateral damage." Cyberspace is, after all, a man-made domain, primarily comprising of infrastructure built, owned, and maintained by private-sector interests for their own ends. Thus the offense-focused cyber activities of states are not being conducted in military isolation, but instead directly interact with the infrastructure that global commerce and domestic industry crucially depend upon.

As an example of the issues that this raises, recall the well-publicized downfall of the Dutch certificate authority DigiNotar. In June 2011, attackers began to compromise sys-

tems at DigiNotar that, as well as being a CA for the private sector, issued Dutch government certificates. By July these same attackers were issuing rogue certificates. In September the sheer scale of the compromise came to light, leaving the Dutch government with little option other than to take over operational management of DigiNotar's systems. Later that month DigiNotar was declared bankrupt. Following lengthy investigation, suspicion fell on the Iranian government for the DigiNotar attack. It appears that the attack objective was to conduct man-in-the-middle attacks against Iranian citizens using rogue DigiNotar certificates.[1]

Although there were many failures in the way DigiNotar handled the incident, the takeaway is that a private sector organization was effectively put out of business in less than four months by the unanticipated actions of a state attacker. Further, while DigiNotar itself was bankrupted, its legacy also had potentially catastrophic implications for its parent company, VASCO Data Security. At the time, it was estimated that VASCO faced losses of up to $4.8 million,[2] but of far greater concern was an unknown liability exposure resulting from its ownership of DigiNotar.

The DigiNotar case also highlights that the motivation for a state attacking a private-sector company is rarely straightforward. In this case DigiNotar was simply a stepping stone to achieving an objective of no concern to the company. There seems little doubt that we will see more private-sector organizations surprised and alarmed to find themselves targets of state adversaries, and in many cases it seems likely that the targets will struggle to make sense of the unwelcome actions. The DigiNotar case also provides a timely reminder that private sector information security professionals are not just responsible for the information assets of the business; they also carry a very real responsibility for the potential survival of the business itself.

1 Fox-IT. Black Tulip - "Report of the investigation into the DigiNotar Certificate Authority breach," 2012 – http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html.

2 Lennon, M., "VASCO: Losses from DigiNotar Bankruptcy under $5 Million, 2011 – http://www.securityweek.com/vasco-losses-diginotar-bankruptcy-under-5-million.

Fallout from state intelligence cooperation

It is not just direct action from state cyber operations that can impact the private sector. We have been treated to a cascading deluge of revelations surrounding the cyber activities of US intelligence services and their global partners in both the public and private sector. As a result, many of the world's biggest names in technology and telecoms have been left with some very difficult questions to answer.

Despite streams of denials of involvement, accusations came thick and fast while private sector organizations tried to distance themselves and restore market confidence. As the scale of cooperation between intelligence services and the US private sector was revealed, many states and businesses around the globe began to view US companies with increasing suspicion. It is safe to assume that these concerns will continue to haunt the companies involved for many years to come, which in turn will impact the US technology sector's ability to compete internationally. Indeed, 2013 estimates suggested that the sector could miss out on anywhere between $22 billion[3] to $180 billion[4] in cloud sales internationally over a three-year period. A tangible example of such private sector loss is the much commented on decision of the Brazilian government to award a $4.5 billion[5] contract to replace Brazil's aging jet fighters to Saab of Sweden, despite Boeing of the US being the clear front-runner throughout the tendering process.

However, it is not just the US that has been exposed by these revelations. Many of its Five Eyes partners (UK, Canada, New Zealand, Australia) were likewise implicated, raising concerns about their national tech sectors. In addition, accusations of interference with products from non-US manufacturers will almost certainly impact the companies concerned and their own domestic economies. And who would bet against us learning of similar behavior by other foreign intelligence services in years to come?

In addition to impact on individual companies there were even more far-reaching disclosures of attempts to undermine entire technologies. Of particular concern were the revelations of well-funded, systematic efforts to undermine cryptography. These revelations culminated in a December 2013 *Reuters* article[6] that raised some very difficult questions for RSA, now part of EMC, about the NSA's ability to influence the integrity of RSA's cryptographic products, specifically its BSAFE toolkit. The impact of this has the potential to seed doubts about the protective capability of cryptographic toolkits. It is thus not inconceivable that the actions of one private-sector organization could have knock-on effects for

3 Castro, D., "How Much Will PRISM Cost the U.S. Cloud Computing Industry?" 2013 – http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry.

4 Staten, J., "The Cost of PRISM Will Be Larger Than ITIF Projects," 2013 – http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

5 Soto, A., "Saab Wins Brazil Jet Deal after NSA Spying Sours Boeing Bid," 2013 – http://www.reuters.com/article/2013/12/18/brazil-jets-idUSL2N0JX17W20131218.

6 Menn, J., "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," 2013 – http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

SAVE $200

Register with priority code GARTISSA

Gartner Summits

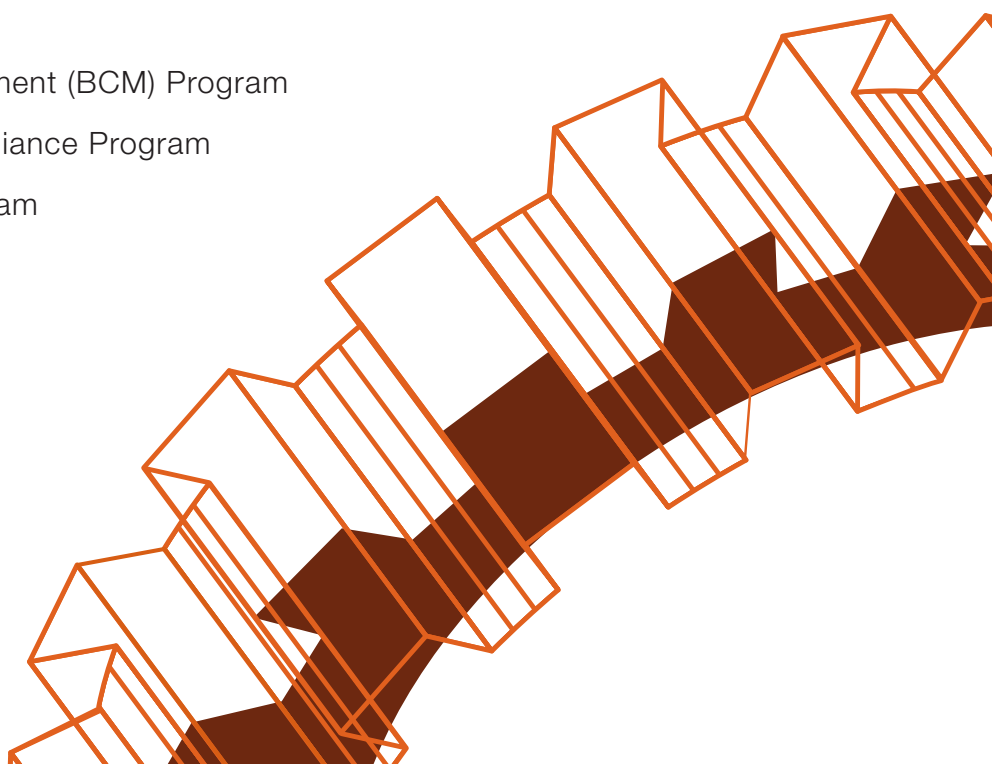
Gartner Security & Risk Management Summit 2015

June 8 – 11 | National Harbor, MD | gartner.com/us/securityrisk

Re-evaluate your security and risk strategies

Discover five role-based programs targeted to your security and risk needs

- Chief Information Security Officer (CISO) Program
- IT Security Program
- Business Continuity Management (BCM) Program
- Risk Management and Compliance Program
- Business of IT Security Program



companies that have not engaged in any cooperative relationships with intelligence services.

The impact of espionage

In January 2009, Nortel, the Canadian multinational telecommunications and data networking equipment manufacturer, filed for bankruptcy. Although the company had other issues, it is believed that sustained espionage significantly contributed to its demise. It appears that attackers had unfettered access to the company's networks for around a decade.

Many Western states assert that cyber espionage is the most significant issue facing the private sector and point to China as a major culprit. While these states portray themselves as victims, critics assert that these states are engaging in many of the same activities. For example, alleged UK operations against Belgacom[7] and US operations against Huawei[8] raise questions as to where exactly the boundaries of national security missions are drawn.

The issues surrounding espionage are complex with semantic, cultural, and historical factors all coming into play. But what is clear is that espionage presents the private sector with significant challenges, many of which are presented by the activities of state actors.

Winners and losers

Historically attackers have always held an advantage over defenders in cyberspace. The vast financial resources that states bring into play on the offensive side mean that attackers will continue to enjoy this advantage. Indeed, if unchecked, that advantage will surely grow.

Like the majority of those working in cybersecurity today, we do not hold any security clearances and are solely informed by open-source intelligence. It is therefore quite difficult to comprehensively assess a given state's actual commitment to cyber offense relative to defense. However, estimates that the US military may be spending up to four times as much on cyber offense research than it does on cyber defense research[9] are of grave concern, particularly as the US model is one that many states globally aspire to emulate.[10]

Another area of particular concern is the stockpiling of zero-day exploits. Markets for zero-days are a major growth area, and states are amongst the newest and best-financed customers. Estimates vary, but it appears that sums of up to $250,000[11] have been paid for quality zero-day exploits on the

7 Der Spiegel, "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm," 2013 – http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

8 Der Spiegel, "Targeting Huawei: NSA Spied on Chinese Government and Networking Firm," 2014 – http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html.

9 Wolfe, J. *Cybersecurity Becomes Central To U.S. Interests*. 2014 – http://www.forbes.com/sites/investor/2014/01/14/cybersecurity-becomes-central-to-u-s-interests/.

10 BBC. *South Korea to develop Stuxnet-like c*yberweapons. 2014 – http://www.bbc.co.uk/news/technology-26287527.

11 Greenberg, A, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," 2012 – http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

black market. The tacit legitimization by states of this activity will undoubtedly ensure that these markets will flourish. In doing so, states may even inadvertently be funding criminal enterprise.

There are, of course, private sector companies gaining from this industry. A new breed of small, specialist firms are specializing in providing states with access to zero-day exploits and other offense-focused tools. As their products reach ever increasing levels of sophistication, so too do the significant ethical and moral issues associated with this trade. For example, a researcher discovering a new zero-day exploit can now choose whether to disclose it and potentially face significant legal, financial, or professional repercussions, or instead sell this knowledge for handsome reward.

This hardly bodes well for the future ability of private-sector manufacturers to identify and address future vulnerabilities in their products.

The way forward

From a private sector perspective, what we are seeing is the rapid erosion of a trust model we have come to depend upon. We trusted our hardware and software manufacturers to ensure that the products that they provided were as secure as they could reasonably make them. We trusted that if security issues were identified, then they would be investigated and addressed. We trusted our standards bodies to guide us in the right direction and to have robust mechanisms for ensuring that the standards they produced were not prone to manipulation. Without these trusted foundations our ability to accurately assess risk, something that is incredibly difficult to do accurately at the best of times, becomes effectively impossible.

The militarization of cyberspace presents us with significant technical and legal challenges, but the biggest challenges of all are political. We traditionally require the state to find the right balance between military, business, and social priorities in cyberspace. Evidence of the recent actions of military actors suggests that this balance is not currently correct. That is not to suggest that the armed and intelligence services of most Western democratic states are in some way intentionally malicious towards the private sector or society as a whole. After all, there are boundaries defined by the state within which subordinates must operate. However, it seems that state governments have not been able to resolve major issues that arise where these boundaries overlap and conflict. This problem is further compounded by military actors who are expected to operate up to and even on these boundaries that quickly widen as technology rapidly advances, but law lags behind. This is something that we are very familiar with in other aspects of information technology: the ongoing tension between law and technology surrounding digital rights management being a prime example.

The irony here is that the true source of a state's power in cyberspace rests not in its military but in the market dominance of its technology private sector. If a state allows militarization to become the embodiment of its cyber capabilities to the exclusion and detriment of its private sector, then it is, in essence, trading influence for the illusory control of a domain that over the long term cannot be controlled. Ultimately states that allow identified vulnerabilities to go unchecked run the very real risk of allowing their capabilities today to become the vectors of criminal enterprise tomorrow.

From a private-sector perspective, it is likely that further militarization of cyberspace will result in the passing of a tipping point. Beyond this we will be sufficiently overwhelmed that, somewhat ironically, we will possibly no longer be able to manage cybersecurity risk without state support. On current trends, the likelihood is that the private sector gets dragged deeper into an offense-driven cyber-deterrence proposition. Another possibility, perhaps almost unthinkable today, is that organizations and individuals will deem it no longer worth the risk to continue operating in cyberspace.

The way forward has only one viable direction. For the private sector as a whole, and information security practitioners in particular, it has become absolutely essential not to focus exclusively on the technicalities of securing our businesses in cyberspace. We must also stand up and actively engage in the political aspects of this challenging problem. This will need critical thinking beyond the confines of individual organizational interests. It will also require proactively challenging the emerging status quo of progressive militarization of cyberspace. We must think well beyond the immediate requirements of our day jobs in order to safeguard society, and our profession, from an unpalatable future.

This article is abridged from an MSc Information Security thesis submitted to Royal Holloway, University of London.

About the Authors

Constantinos Macropoulos holds an MSc in Information Security from Royal Holloway, University of London. He has almost two decades of private-sector experience, working in a diverse range of IT roles including operations, deployment, design, and compliance. Over this time he has developed a keen interest in the dynamics between state and private-sector interests surrounding information technology. He may be reached at macro@greenhatlabs.com.

Keith Martin is a professor in Information Security and director of the Information Security Group, Royal Holloway, University of London. He is the author of the recently published Everyday Cryptography by Oxford University Press. As well as conventional teaching, Professor Martin is a designer and module leader on Royal Holloway's distance learning MSc Information Security program and regularly presents on cybersecurity topics to industrial audiences and schools. He may be reached at Keith.Martin@rhul.ac.uk.