eSeminar Summary

Centre for Security Governance | No. 3 | September 2014

The Centre for Security Governance eSeminars bring together leading security sector reform experts to discuss a range of SSR-related issues and cases on a quarterly basis.

Centre for Security Governance

New Frontiers in Security Sector Reform: Countering Technology-Driven Threats

Introduction

With the burgeoning use of cyberspace and digital applications, individuals, private companies, and governments have all become increasingly concerned about the dangers of attacks that target the cyber domain. Cyber attacks involve the "access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information."[1] Of course, the purposes of such attacks can vary quite widely – from cyber vandalism by hacker anarchists to cyber terrorism and cyber crime committed by more organized groups to the type of cyber warfare and espionage normally associated with states.

Cyber security measures designed to mitigate or respond to such technology-driven threats have traditionally been a focus for more developed countries, which enjoy greater connectivity, advanced information and communications technology (ICT), and a greater sense of vulnerability to disruption or damage. One need only consider the Pentagon's recently established Cyber Command, expected to grow to a 6,000-strong force with "full spectrum cyber capabilities."[2] Meanwhile, Russia has deployed a vast cyber surveillance network with its SORM (System of Operative-Investigative Measures) system, and strengthened its cyber warfare capabilities.[3] China is also suspected of being behind cyber espionage directed against Western targets, both state and private sector. The United States has even taken the unprecedented step of indicting five Chinese military hackers accused of such activities.[4]

Yet the cyber domain is also a growing concern for developing countries as well, which can all too easily become targets of cyber attacks. For example, Iran found itself on the receiving end of a sophisticated computer virus – Stuxnet – reportedly sent by the United States and Israel to disrupt its nuclear program. Countries like Georgia and Estonia have borne the brunt of cyber attacks originating from Russia. Kenya has been one of the worst affected countries in the world when it comes to cybercrime, for instance. In 2013, 5.4 million cyber attacks were detected in Kenya's cyberspace, a 108 percent increase from the previous year[5] (see Box 1 for an overview of the scale of Kenya's cyber security theat and the government response). Developing countries have also offered fertile ground for cyber criminals capable of threatening developing and developed countries alike. With Internet penetration levels already quite high in the developed world, much of the growth in Internet usage is expected to come from the developing world and especially Africa, where four-fifth of the continent's population lacks Internet access.[6] This only increases the urgency of exploring cyber security's place in security sector reform (SSR) in order to ensure that donor assistance to developing and transition states adequately accounts for cyber vulnerabilities and future threats.

On July 17, 2014, the Centre for Security Governance organized an eSeminar that brought together three distinguished observers to examine cyber security and its potential place

About the eSeminar Series

The Centre for Security Governance eSeminars are a series of virtual meetings that bring together experts and practitioners from around the world to discuss security sector reform (SSR) and related themes, issues, and case studies. The eSeminars are open to the public, and includes three key components: the eSeminar Primer, eSeminar Summary, and eSeminar Videos. For information on upcoming eSeminars, please visit http://www.secgovcentre.org/events.

Series Editor: Mark Sedra
Report Author: David McDonough

About the CSG

The Centre for Security Governance is a non-profit, non-partisan think tank dedicated to the study of security transitions in fragile, failed and conflict-affected states, a process also known as security sector reform. A registered charity based in Kitchener, Canada, the CSG maintains a global network of research fellows from a variety of backgrounds, including practitioners, research analysts and academics, and partner organizations from the public and private sector engaged in SSR.

Centre for Security Governance
Tel: +1 226 241 8744
Email: info@secgovcentre.org
Web: www.secgovcentre.org
SSR/RC: www.ssrresourcecentre.org

Box 1: Cyber Security in Kenya

Kenya is currently ranked as one of the top countries for incidents of cyber crime, according to the Kenya Cyber Security Report 2014 compiled by the Serianu Cyber Threat Intelligence Team. As a result, the country is reportedly losing upwards of US $23 million annually to cyber criminals who have increasingly targeted Kenya's ICT infrastructure. Bank fraud is considered an area of particular concern. While emblematic of the cyber criminality on the continent, Kenya has also moved to strengthen its own cyber security capabilities.

As early as 2011, the country was one of the few in East Africa to set up a Computer Incident Response Team. Following the 2013 launch of its National Cyber Security Master Plan, the government began a process to formulate a comprehensive cyber security strategy. The end result was unveiled in June 2014 with the Kenya National Cybersecurity Framework in 2014, consisting of The National Cybersecurity Strategy, the National Public Key Infrastructure (NPKI), and the National Kenya Computer Incident Response Team – Coordination Centre. Its draft Cybercrime and Computer Crimes Bill, expected to be tabled by parliament this year, will empower its judiciary to go after Kenyans implicated in cyber attacks, even outside the country. Other noteworthy initiatives include the creation of a special investigative cyber crime unit within the Office of the Director of Public Prosecutions.

Sources: Charlie Fripp, "Kenya creates special cyber-crime unit," *IT News Africa*, 19 January 2014, http://www.itnewsafrica.com/2014/01/kenya-creates-special-cyber-crime-unit/; Daily Nation, "Tough law on cybercrime targets all Kenyans," 18 June 2014, http://mobile.nation.co.ke/news/cybercrime-Bill-Kenyans-around-the-world-prosecution/-/1950946/2352702/-/format/xhtml/-/by67iyz/-/index.html; Dennis Mbuvi, "Kenya launches National Cyber Security Strategy and Master Plan," CIO East Africa, 12 February 2013, http://www.cio.co.ke/news/main-stories/kenya-launches-national-cyber-security-strategy-and-master-plan; News24 Kenya, "Cyber security framework set for launch," 24 June 2014, http://m.news24.com/kenya/National/News/Cyber-security-framework-set-for-launch-20140624; Rajab Ramah, "Cybercrime on the rise in Kenya," Sabahi, 24 June 2014, http://sabahionline.com/en_GB/articles/hoa/articles/features/2014/06/24/feature-01; Susan Mwenesi, "Kenya ranked amongst top countries globally for cybercrime," humanipo, 12 June 2014, http://www.humanipo.com/news/45024/kenya-ranked-amongst-top-countries-globally-for-cybercrime/; Vincent Matinde, "Kenya government unveils cyber security strategy," *IT Web Africa*, 2 May 2014, http://www.itwebafrica.com/ict-and-governance/256-kenya/232830-kenya-government-unveils-cyber-security-strategy.

in SSR programming in the developing world. Particular attention was paid to the threat of cyber crime, due not least to the prevalent role of cyber criminals in the developing world. The panelists sought to answer some of the key questions about this emerging domain. Specifically, what is the nature of the cyber threat among developing countries? And how should international donors provide SSR assistance in a manner that adequately reflects these technology-driven threats?

Summary of Presentations

Ken Taylor – Towards a Proactive Cyber Posture

The International Cyber Security Protection Alliance (ICSPA) seeks to bring together governments, non-governmental organizations, and corporations from developed and developing countries to share information on cyber crime and facilitate discussions on the benefits of a proactive cyber security stance. According to ICSPA President Ken Taylor, this task will increasingly need to take into account the developing world, due not least to the region's expanding

ICT infrastructure and burgeoning connectivity, whether measured in terms of high speed broadband, mobile phones, social media, or cloud computing.

Improvements in ICT carry the promise of potential economic growth in the developing world. Taylor points to online banking as a particularly important "focus area in many developing countries." At the very least, ICT will allow these poor or fragile countries to leverage the Internet to connect themselves more fully to the global economic system. Yet ICT also comes with a downside. Without the right regulatory regimes, enforcement tools, public education systems, and training infrastructure in place, such expansive connectivity growth potentially exposes these countries to the threat of cyber criminality. For example, criminals can use developing nations' infrastructure as a site for virtual money laundering and a staging ground to launch distributed denial of services (DDOS) attacks, zero-day exploits, and other cyber attack tools/methods.[7]

The ICSPA advocates a cyber security framework drawn from the organization's many years of experience working with both military and commercial partners and assessing similar frameworks emerging from the United States, Canada, and the United Kingdom. This framework entails four key elements: (a) assets; (b) technology; (c) awareness, education, and training; and (d) proactive cyber posture.

First, governments and private organizations need to identify and prioritize their key assets. For instance, a bank's key asset might be client information and its secondary asset internal infrastructure. Once prioritized, up-to-date technology should be employed to protect these assets, now and into the future. Continuing with the example of the bank, if the key asset is client data, Taylor recommends "multi-factor authentication" and "encryption technology" as protection. While Taylor uses the example of private banks, both points can easily be extended to discussions about a developing or transition state's security sector. For instance, law enforcement agencies would need similar technological safeguards to protect their own assets, including personnel information, infrastructure, and criminal databases. Of course, this does not mean that all forms of asset protection require equally sophisticated technology, especially since poorer countries might not have the resources for such measures – the key point is to ensure that assets are protected.

Taylor also points to awareness, education, and training as being integral to a robust cyber security framework. Awareness starts at the internal level, and can include many different mediums to deliver content to an organization (e.g., online documents, video, weekly or even daily meetings). An awareness campaign also needs to keep in mind the rapid pace of technological change, in which "every millisecond something in the world is changing from a technology perspective." This can easily open up new avenues for both cyber protection and threat.

Closely tied to awareness are education and training. For example, while banks today might identify and prioritize their assets and in some cases understand technology, they often lack education and training in cyber security. The same can also be said of developing security sectors, which are often focused on more fundamental issues –such as basic training, institutional reform, anti-corruption, and procurement – and have little time or resources for more specialized cyber security training. Yet some developing countries are starting to treat cyber security more seriously. For instance, Kenya recently established a dedicated cyber crime unit and unveiled a National Cyber Security Master Plan.[8] This example will likely only serve as a harbinger of things to come on the continent, especially in light of the African Union's passage of its first convention on cyber security.[9]

Lastly, Taylor points to the need for a proactive cyber posture, by which he means that organizations should constantly be testing their systems in order to identify gaps, vulnerabilities, and potential threats. This can be done externally, by engaging third-party organizations to test cyber defences, or internally by having key internal actors send out internal phishing emails or adopting reward programs for proactive employees.

Jeffrey Carr – The Strategic Key to Cyber Security

Governments must collaborate on matters of cyber security to protect themselves from cyber attacks against their critical infrastructure. Jeffrey Carr makes this point very directly when he points out that the "violent disruption of major financial, telecommunications, energy, and transportation sectors serve no one." Indeed, governments should recognize that the worst threats actually come from chaotic non-government actors, which have no allegiance other than to cause maximum disruption and harm.

If one is to ensure cyber security, the "strategic key" is to identify those terrorists, anarchists, religious fanatics, and nationalist extremists most inclined and increasingly capable of undertaking cyber attacks. Indeed, these groups are often located among fragile or conflict-affected states in the global periphery, thereby making the question of security and justice reform of these states an important element of dealing with the non-state cyber threat. Common ground needs to be found in order to facilitate inter-governmental collaboration against non-state cyber threats. Unfortunately, the United States seems much more intent on tackling cyber threats from technologically advanced states, thereby forestalling any real great power cooperation against the non-state cyber threat.

A good example is how the United States confronts China. To be sure, the US government and business leaders agree that the sheer scope of China's cyber espionage efforts is enormous. Defence officials are particularly worried about the pace of China's technologi-

cal acceleration and an increasingly powerful Chinese presence in the Asia-Pacific. Yet these efforts to combat China's cyber espionage amounts to what Carr labels a "fools errand" – one that ignores Washington's limited ability to coerce China into stopping such activities and overlooks the hypocrisy of attempting to do so. Much like those in China, American intelligence agencies also "do what is necessary to secure position, safety, sustainability of its power and presence in the world."

Rather than trying to fumble around to stop China's theft of high value technology, it would be more prudent for the United States to seek ways to collaborate with Beijing. It begins by going back to diplomatic basics in order to search for common ground that could result in positive-sum gains for both sides. One possible avenue is China's own domestic problem of hackers, many of whom are suspected to originate from within mainland China (including Tibet) and Taiwan, as well as further afield in India and Korea. Indeed, despite its so-called "Great Firewall," China reportedly suffered 500,000 cyber attacks in 2011 alone.[10]

The US Federal Bureau of Investigation (FBI) has a long history of collaborating with foreign law enforcement agencies to identify and arrest hackers and other cyber criminals, including embedded agents in countries as diverse as "Estonia, Ukraine, Romania, Colombia, and the Netherlands."[11] Some level of collaboration could potentially work in dealing with China's own hacker problem, thereby yielding some useful intelligence about these little known groups.[12] The same can also be said of developing countries. Indeed, in many of these states, donors are already often heavily involved in areas such as law enforcement capacity building and justice reform – so it might be prudent to tailor such SSR programming to better facilitate future collaboration on cybersecurity and intelligence. With human-driven cyber security intelligence sources sorely lacking, international collaboration with such countries could help gather "all-sourced" (signals and human) intelligence on this critical issue. It is critically important for governments to identify the source of a cyber attack, as attribution is key if the state is to weigh its options and pursue a response.[13]

Tim Maurer – Cyber Security in Developing Countries

By the end of 2014, three billion people are expected to be able to access the Internet, the majority either in the developed world or more developed parts of Asia.[14] Another five billion are without access, largely in the developing world. As Tim Maurer notes, differences between developed and developing countries do not end there. For example, users rely on a wide infrastructure to access the Internet in the developed world, while those in developing nations often access the Internet through mobile phones.

Keeping in mind these important distinctions, an assessment of cyber crime in the developing world needs to take into account both the "target of crime" and the "source of crime." In the former, cyber crime today has an inordinate impact on the developed world. However, the share of the burden for developing countries will in all likelihood grow, considering current projections of an additional two billion people accessing the Internet over the next five years. Much of this new connectivity will occur in Asia, which will likely make the region a focus for international assistance and awareness raising. In terms of the sources of cyber crime, the differences in Internet access between developed and developing countries are less salient: so long as a sufficient number of people "know what to do and [know] how to use infrastructure for criminal purposes." Unfortunately, the barriers to entry for cyber crime are low compared to other criminal activities.

The range of possible cyber crime activities is large – from an unsophisticated phishing scheme to a non-state actor potentially hacking into and taking control over power grids for purposes of blackmail (or simply to cause damage and disruption). Of course, more sophisticated attacks would require greater capacity to carry out. Yet it would be a mistake to underestimate the potential cyber capabilities of non-state actors; Mexican drug cartels and Islamist terrorist organizations like al-Qaeda and the Islamic State are good examples.

Internationally, the debate on cyber security turns around definitional issues of what cyber security actually means and entails. One view sees cyber security as information security – a definition that would include threats capable of undermining a state's social stability and would therefore make control of content a key element. It is perhaps not surprising that this view finds favour with Russia and China. As Maurer goes on to say, it quickly turns any cyber security discussion into a "Trojan horse" for possible human rights issues, such as the state's surveillance of and intrusion against "individual citizens for purposes of spying and monitoring." The other definition, used by the US and Europeans (and preferred by Maurer), excludes the issue of content and content manipulation. This shifts the cyber security discussion towards the issue of attacks against critical infrastructure.

Maurer's final point concerns the issue of asymmetry between developed and developing countries. Developed countries can be considered more vulnerable than developing countries, due to the prevalence of Internet access and devices. More devices can potentially be hacked and the consequences of cyber attacks could be more severe. Yet the developing world is more vulnerable in certain key areas. After all, they might lack the latest technologies or find themselves unable to benefit from the latest cyber defences deployed by their more developed peers. In some respects, their lack of cyber sophistication could offer an advan-

tage, such as when their lack of connectivity minimizes and localizes the impact of a cyber attack. Of course, these countries are also left vulnerable by a lack of resilience. With fewer redundancies, developing countries have much less ability to respond to a cyber incident.

Issues and Themes

The eSeminar concluded with a question-and-answer discussion moderated by the CSG Executive Director Mark Sedra, which raised key issues and themes relevant to the issue of cyber security.

International Cyber Security Assistance

Much like with SSR, international cyber security assistance needs to focus on training and capacity building, with a special emphasis on resilience. Tim Maurer notes that capacity in many of these countries is often severely lacking. A key challenge will therefore be to make sure people have the technical expertise and capacity to address cyber threats. Sadly, it is often insufficient to briefly train people on cyber security and assume that such skills will continue to be relevant over the next decade or two. Technology, applications, and platforms are rapidly changing in the cyber security field. Donors should seek to establish continuing educational programs for the security institutions of partner countries, notably police forces and justice agencies that would be the sharp end of any effort to deal with cyber crime. Only then can partner countries and possess the latest technologies and best practices to confront the growing cyber security challenge.

Yet international cyber security assistance also leads to other questions – namely, who exactly is going to be a partner to build bridges and advance collaboration on cyber security? Within the broader UN system, Maurer notes that the International Telecommunications Union (ITU) has traditionally played a focal point role on the issue of cyber security. Yet today, the ITU is widely seen as being dominated by the views of Russia and China, in which cyber security is seen primarily through the informational security lens. The ITU itself also lacks any operational on-the-ground programs. Instead, it must work through the representatives of the United Nations Development Program.

An alternative to the ITU is either bilateral assistance programs or a different intergovernmental organization. Maurer recommends focusing on existing bilateral ties. Yet, as Jeffrey Carr notes, the Edward Snowden revelations about the US National Security Agency's cyber-snooping, often in collusion with the private sector (knowingly and unknowingly), have cast a shadow on the US government and its technology giants. Given the ensuing and understandable distrust, countries may and perhaps should be reluctant to rely on one source – irrespective of whether it is the US or other large technical assistance donors – for the development of their ICT and Internet security infrastructure.

It is difficult to underestimate the role of trust in facilitating collaborative cyber security efforts. An important step was the 2004 Budapest Convention on Cybercrime, which addresses a variety of cyber criminal acts (e.g., copyright infringement, electronic fraud) and already has 50 member countries, of which 42 have ratified the agreement. Ken Taylor also points to the role of global non-profits like ICSPA in conversing with Caribbean leaders in forums, conferences, and working groups, which helped build the trust necessary to establish the Caribbean Cyber Security Center.[15]

Cyber Security and Resilience

Resilience is a critical component to safeguard assets against cyber threats. As Jeffrey Carr notes, it was discovered that the US Department of Defense had critical assets reliant on an otherwise vulnerable public power grid, with only a few days of backup power if the system ever went down. In response, the United States moved to create a back-up system composed of solar-powered micro-grids, which were independent of the public grid and used more secure and modern software and hardware systems.[16] As he goes on to say, "building in resilience early is critical…to keep your infrastructure up and running."

Both Ken Taylor and Tim Maurer also reiterate the important of resilience. Taylor points to the need for proactive senior-level involvement in order to ensure that all key parties – whether internal or external third-party actors – are working collaboratively to test their systems' resilience. Maurer agrees that "backup systems must be in place." Yet he also sounds a warning that cost remains an important factor for any actor, whether government or private industry. Simply put, the cost of developing an advanced and totally independent backup system would be exorbitant, particularly in developing world security sectors.

Yet Maurer also raises an interesting alternative to internal backup systems – namely, cooperative arrangements between actors. In the case of an attack, one would then have the option of using the resources from its partner as a temporary backup. An illustrative example is when the Georgian government relied on an American company in Florida to host its website after suffering a massive DDoS attack. Public-private partnerships could also entail the integration of security measures to protect ICT infrastructure.[17]

Admittedly, such arrangements can also be a particularly sensitive issue. Corporations will likely be eager to protect their proprietary information and client data against potential state cyber snooping, just as governments would be equally hesitant to involve the private sector, especially on cases that can impinge on national security – such as backup arrangements for ICT systems used by the state's law enforcement agencies or military. Still, both corporations and states share a common interest in

combating cyber threats and will likely need to cooperate to better safeguard their networks and ICT infrastructure.

Cyber Crime and Technology-Driven Threats

Several developing or transition countries have increasingly become sanctuaries for hackers and other cyber criminals, whether due to their lack of effective law enforcement and governance capacity or their interest in leveraging domestic hackers to attack targets abroad. Former US presidential special advisor on cyber security Richard Clark has singled out post-Soviet states as being particular culprits, especially Russia, Belarus, and Moldova. Yet there are few geographic constraints to "cyber-sanctuaries," with other safe havens ranging from Nigeria and Ghana to Brazil and China.[18]

Yet empirical data on the exact scale of the cyber security threat is, as Maurer acknowledges, much "harder to come by." It also helps to distinguish between intrusions and cyber attacks when discussing any cyber incident. To initiate a cyber attack, an individual or group must first gain access to a system – e.g., by taking advantage of a system's vulnerability. This is commonly called an intrusion. Only when you gain access can you undertake an attack by releasing a payload. As Maurer goes on to say, "when we hear very large numbers, it usually refers to the probing or intrusion of a system."

DDoS is a particularly common form of cyber attack. It essentially leverages the computers, smart phones, or any Internet-enabled device from multiple users, who might not even know that their systems have been hijacked. Such devices are turned into "zombie machines" through a particular virus or malware. Multiple zombie machines are formed into a network controlled by a single user or entity, thereby becoming what is called a "botnet." All the devices are used to send out requests to a specific website simultaneously, thus overloading the capacity of the targeted infrastructure and making it vulnerable to attack. The potential of botnet-launched DDoS attacks is particularly alarming in light of the developing world's growing embrace of the Internet.

According to Ken Taylor, an important determinant of a country's vulnerability to cyber crime and cyber threats is its law enforcement capacity. A good example can be found in the Caribbean, which is one of the most targeted regions of the world in terms of cyber crime – due largely to its lack of law enforcement capacity, whether measured in terms of resources allotted, skewed policy priorities, or the resultant scale of crime. Another determinant is also the size of the country and the extent to which it is wired. As Carr notes, countries that are small, highly wired, and heavily reliant on Internet for daily life – a good example being Estonia – are particularly vulnerable to DDOS that could shut down their connectivity and cause serious disruption for a sustained period of time. Larger countries like the United States

are much harder to disrupt owing to their multiple points of connectivity.

Jeffrey Carr says that terrorist and extremist groups are already using the Internet for training, recruitment, propaganda, and communications purposes – so a cyber terror attack cannot be discounted. One potential harbinger is the foiled cyber attack on the Nasdaq by Russian gangs.[19] Another is the growing number of hackers flocking to one side or another of the Syrian-Iraqi civil wars, such as the Syrian Electronic Army in support of President Bashar al-Assad (possibly with direct links to the regime itself) and ISIS Cyber Army coalescing in support of the Islamic State insurgents.[20] Al-Qaeda itself has followed this trend, with groups like the Tunisian Cyber Army and al-Qaeda Electronic Army now associated with them.[21] Still, Maurer also sounds a more cautionary note by pointing out how talk of cyber terrorism has since shifted to what is now called the "terrorist use of the Internet" – in recognition that the cyber domain is still *predominantly* used as a communication tool for terrorists.

Conclusion

Developed countries clearly field the most advanced cyber capabilities today. Yet, as their Internet use grows, developing countries are destined to play a growing role in this cyber security arena. On one hand, hackers intent on committing cyber attacks – whether individuals, terrorist/criminal syndicates, or even state-sponsored groups – will assuredly seek to leverage the growing number of potentially vulnerable Internet devices in these countries, making the developing world a fertile enabler for botnets and DDoS attacks. On the other hand, many developing states also lack the security sector and law enforcement capacity to adequately deal with such cyber criminality. With their Internet connectivity set to grow, this makes developing countries increasingly vulnerable, whether as a source of a cyber attacks or as a possible target.

Cyber security resilience needs to be advanced as an integral component of donor SSR assistance to developing countries. Backup networks for telecommunications, transportation, and the power grid need to be prioritized. Law enforcement agencies also need to be strengthened and directed to deal with cyber criminals, in order to prevent these countries from becoming ungoverned cyber sanctuaries. Indeed, a "whole of society" approach should be adopted. As Tim Maurer notes, a potentially useful analogy for dealing with viruses, malware, and other cyber threats might very well be global health, in which multilateral institutions, governments, and the private sector must work closely together. Yet donors need to recognize the unique educational challenges in providing assistance in a constantly and rapidly evolving technological domain like cyber security. Assistance needs to be sustained and long-term, so that security sector and governance institutions are fully prepared to deal with this 21st century threat.

About the Presenters

Ken Taylor is currently the President of the International Cyber Security Protection Alliance (ICSPA) for The Americas. He is also the CEO of InnovaNord and is recognized as a global cyber security leader.

Jeffrey Carr is the author of "Inside Cyber Warfare: Mapping the Cyber Underworld" (O'Reilly Media 2009) and the founder and CEO of Taia Global, Inc., a boutique security consulting firm for Global 2000 companies.

Tim Maurer focuses on cyberspace and international affairs at the New America Foundation. He is part of New America's Future of War project and the Research Advisory Network of the Global Commission on Internet Governance.

Notes

1. Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Government of Canada, 2010,) p. 3.

2. Ellen Nakashima, "U.S. cyberwarfare force to grow significantly, defense secretary says," *The Washington Post*, 8 March 2014, http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html.

3. Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* (Fall 2013), http://www.worldpolicy.org/journal/fall2013/Russia-surveillance; Jeffrey Carr, "Russian Cyber Warfare Capabilities in 2014 (We aren't in Georgia anymore)," *Digital Dao*, 8 March 2014, http://jeffreycarr.blogspot.ca/2014/03/russian-cyber-warfare-capabilities-in.html.

4. Andy Greenberg, "U.S. Indictment of Chinese Hackers Could Be Awkward for the NSA," *Wired*, 19 May 2014, http://www.wired.com/2014/05/us-indictments-of-chinese-military-hackers-could-be-awkward-for-nsa/.

5. Paula Kigen et al., *Kenya Cyber Security Report 2014* (Nairobi: Serianu Limited, 2014).

6. UN News Centre, "Internet well on way to 3 billion users, UN telecom agency reports," 2 May 2014, http://www.un.org/apps/news/story.asp?NewsID=47729#.U_Y_SpUg_X4

7. DDoS attacks are designed to overwhelm servers and crash systems and websites. In contrast, zero-day exploits are meant to take advantage of coding errors before a vulnerability is known and a software patch is released. Other commons weapons and methods for cyber attacks include viruses, worms, trojans, and logic bombs. For a good overview, see Scott Shackleford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (New York: Cambridge University Press, 2014), pp.136-144.

8. Vincent Matinde, "Kenya government unveils cyber security strategy," *IT Web Africa*, 2 May 2014, http://www.itwebafrica.com/ict-and-governance/256-kenya/232830-kenya-government-unveils-cyber-security-strategy; Charlie Fripp, "Kenya creates special cybercrime unit," *IT News Africa*, 19 January 2014, http://www.itnewsafrica.com/2014/01/kenya-creates-special-cyber-crime-unit/.

9. News from Africa, "Africa Union Convention On CyberSecurity And Personal Data Protection," 23 June 2014, http://www.newsfromafrica.org/newsfromafrica/articles/art_14335.html.

10. Paul Harris, "Chinese army hackers are the tip of the cyberwarfare iceberg," *The Guardian*, 23 February 2013, http://www.theguardian.com/technology/2013/feb/23/mandiant-unit-61398-china-hacking.

11. Richard Weitz, "The FBI and Cyber Defense," *Second Line of Defense*, 18 May 2011, http://www.sldinfo.com/the-fbi-and-cyber-defense/.

12. On this issue, Jeffrey Carr does note that he is not differentiating between the actions conducted by inde-

pendent hacker groups and those conducted with state support/direction.

13. The same cannot be said of corporations. As Carr notes, for them, it is irrelevant whether an attack "is coming from Korea, China, Russia, Germany [or] Israel," since the assets and resources necessary for defence would be the same regardless. Instead, corporations should adopt a data-centric approach, where the focus is less about keeping dedicated attackers out and more about ensuring that network assets are sufficiently difficult to access, copy, or steal, in what Carr calls an "assumption of breach" paradigm. For more on this paradigm, see Jeffrey Carr, *Assumption of Breach: The New Security Paradigm* (Sebastopol, CA: O'Reilly Media, 2014).

14. UN News Centre, "Internet well on way to 3 billion users, UN telecom agency reports," 2 May 2014, http://www.un.org/apps/news/story.asp?NewsID=47729#.U_Y_SpUg_X4

15. For further information, see Barbados Underground, "Caribbean Cyber Security Centre Launched In Barbados," 16 March 2013, http://barbadosunderground.wordpress.com/2013/03/16/caribbean-cyber-security-centre-launched-in-barbados/.

16. For more information on these micro-grids, called Smart Power Infrastructure Demonstration for Energy Reliability and Security, see Tina Casey, "In First Test, U.S. Military's SPIDERS Microgrid Uses 90% Renewable Energy," *CleanTechnica*, 12 February 2013, http://cleantechnica.com/2013/02/12/u-s-militarys-new-spiders-renewable-energy-microgrid/.

17. Rajab Ramah, "Cybercrime on the Rise in Kenya," *Sabahi*, 24 June 2014, http://sabahionline.com/en_GB/articles/hoa/articles/features/2014/06/24/feature-01.

18. Phil Muncaster, "Former White House advisor urges action on 'cyber sanctuaries,'" *V3.co.uk*, October 13, 2010, http://www.v3.co.uk/v3-uk/news/2001245/former-white-house-advisor-urges-action-cyber-sanctuaries; Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security," in *Virtual Battleground: Perspectives on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Netherlands: IOS Press, 2009), pp. 92-93; Walid Khefifi, "Cybercrime: huit pays africains « fichés » parmi les plus risqués de la planète," *Agence Ecofin*, September 14, 2013, http://www.agenceecofin.com/securite/1409-13605-cybercrime-huit-pays-africains-fiches-parmi-les-plus-risques-de-la-planete.

19. Michael Riley, "How Russian hackers stole the Nasdaq," *Business Week*, 17 July 2014, http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq#p1.

20. Nicole Perlroth, "Hunting for Syrian Hackers' Chain of Command," *New York Times*, May 17, 2013, http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=1&; "The ISIL / ISIS Cyber Army and other hacking groups," *Cyberwarzone*, July 3, 2014, http://cyberwarzone.com/isil-isis-cyber-army-hacking-groups/.

21. Terrorism Research and Analysis Consortium, "Tunisian Cyber Army and Al-Qaeda Electronic Army," http://www.trackingterrorism.org/group/tunisian-cyber-army-and-al-qaeda-electronic-army.