



BOSTON GLOBAL FORUM REPORT

CYBERSECURITY

2016

Boston Global Forum
Beacon Hill
Boston, MA 02108

12/12/2015

ABSTRACT

With the exponential growth of the information economy since the 1990s, cyber-security has become a top priority for governments and industry world-wide. This report predicts major cyber-security issues for 2016. While cyber-security measures continue to evolve positively, cyber-threats from crime, terrorism, militarization, espionage, and censorship will continue or worsen in 2016. Conflict over cybersecurity will increase between the West, and criminals and states from which cyber-threats emanate, including terrorists, China, Russia, Iran, North Korea, India, Pakistan, Brazil, Argentina, and many developing countries. Increasing technical sophistication and vulnerabilities in critical infrastructure, military systems, industrial control systems, the internet of things (IoT), machine-to-machine (M2M) communications, and mobile platforms will increase opportunities for states, criminals, and thrill-seekers to discover zero-day vulnerabilities and benefit from cyber tactics. Individualized encryption and the use of crypto-currencies such as bitcoin will continue to facilitate anonymous crime and terrorism, and thereby complicate the cyber-security landscape in 2016. Secure backdoors for legitimate governance and additional regulation of crypto-currencies is necessary. The lack of cyber-security budgets has created labor market shortages in cyber-security, leaving most small countries and mid-sized companies lagging well behind a growing army of cyber-criminals. As cyber-security budgets increase in 2016, so will the incentives to enter the cyber-field. As cyber-security hiring often comes from hackers, hacking conferences, and even cyber-criminal communities, increased budgets are a double-edged sword that may also provide a pull-factor for new hackers. Protecting governments and economies from these threats will require increasing the treatment of cyber-security as a public good, increasing cyber-security budgets in a smart manner, and strong public-private partnerships for provisioning codes of conduct, mandatory information sharing, law enforcement, defense, industrial control system (ICS) security, and non-subsidized cyber-insurance. International agreements on cyber-security will be necessary to properly incentivize countries to prosecute cyber-criminals within their borders, and disincentivize their own use of cyber-tactics for war and espionage. For responsible governance, sometimes the best defense is a good offense – governments need to increase efforts to find, fix, and finish cyber-criminals and terrorists in order to decrease the costs of often ineffective cyber-defenses. Voluntary codes of ethics and privacy technologies will be necessary to discourage slander and the invasion of privacy by hackers and governments, and encourage responsible use of the internet by citizens.

BOSTON GLOBAL FORUM

Boston Global Forum (BostonGlobalForum.org), a public policy think tank, gathers thought leaders to inspire creative and practical collaboration on solving problems that affect the world.

Founded in December 2012, Boston Global Forum includes former Massachusetts Governor Michael Dukakis; John Quelch, the Charles Edward Wilson Professor of Business Administration at the Harvard Business School; Thomas Patterson, the Bradlee Professor of Government and the Press and acting director of the Shorenstein Center on Media, Politics, and Public Policy at Harvard Kennedy School; and Nguyen Anh Tuan, founder of media companies in Vietnam and Chair of the International Advisory Committee on Global Citizenship Education at UCLA.

Table of Contents

ABSTRACT	1
BOSTON GLOBAL FORUM.....	2
INTRODUCTION	4
CYBER-THREATS	4
Crime.....	7
Hacktivism.....	9
Case Study of the Virtualization and Anomie of Youth: Twitch and Swatting.....	11
Terrorism	13
Definition of Cyber-Terrorism	14
Terror Groups that use Cyber Tactics.....	15
State Cyber-Tactics: Militarization, Espionage and Censorship	19
High-Threat Countries	21
China.....	21
Russia	22
Iran.....	23
North Korea	23
Brazil.....	24
India and Pakistan.....	24
Developing Countries	25
CYBER-THREAT TRENDS.....	26
The Internet of Things	26
Blastware, Ghostware, Ransomware, Onion Attacks, and Evoware	26
The Encryption Battle	27
HUMAN SOLUTIONS TO CYBER-RISKS.....	29
Legal Solutions	30
Policy Solutions.....	31
CONCLUSION	35

INTRODUCTION

Dramatic technological advancement over the course of the last two centuries has concurrently widened and enmeshed the global online domain, effectively introducing cyber threats as an issue for state and non-state actors alike. The invention of the computer brought untold benefits across every conceivable sphere, including the social, technological, and cultural. Yet as long as cyber-technology proliferates, so do vulnerabilities. The very progress of digital technology is the creation and broadening of technological surfaces upon which antagonists can search for new zero-day exploits. The year 2016 will be a year of continued cyber-innovation, and with it, increasing cyber-threats, including from crime, terrorism, militarization, espionage, misuse of the internet, and censorship. All will necessitate a global, forward-looking, and layered security response to protect communities and commerce from the new and as-yet inconceivable.

CYBER-THREATS

In this study, we cover five major types of cyber-threat: crime, terrorism, militarization, espionage, censorship, and misuse. While censorship is not normally covered under the rubric of cyber-security, we posit that the ubiquity of communication online has given rise to new government cyber-tools that threaten citizen lives, privacies, and freedoms in ways not heretofore seen.

We use a Merriam-Webster Dictionary definition of hacker: “a person who illegally gains access to and sometimes tampers with information in a computer system.”¹ These are also known as “black hats.” While many hackers and computer security professionals argue that “penetration testers,” “ethical hackers,” or “white hats” should be distinguished from “black hats”, we agree and disagree. We agree in that we wish to distinguish penetration testers from hackers by calling them computer security experts or penetration testers. But we disagree with the term “ethical hacking” for being oxymoronic and leading to self-justification, confusion, and moral subjectivity. Many Islamic State hackers, for example, would likely consider themselves “ethical hackers” if given the choice of calling themselves ethical or unethical hackers. We doubt many hackers would call themselves unethical hackers, for most of them likely have self-justifying reasons for their hacking.

A new website, haveibeenpwned.com, is a useful initial illustration of a number of themes we will discuss throughout this study. At haveibeenpwned.com, anyone can check his or her email address against the millions of email addresses that hackers have publicly released. The website is an innovation, and every innovation produces value but also cyber-risk. Second, it shows the magnitude of the problem. We reproduce as Figure 1 a graph from haveibeenpwned.com, listing the top 10 breaches by number of accounts released. The biggest

¹ Merriam-Webster Dictionary, “Hacker”, accessed 12/8/2015, <http://beta.merriam-webster.com/dictionary/hacker>.

was Adobe in 2013, which lost 152 million emails and passwords.² This year, Ashley Madison (the website for people seeking affairs) lost 37 million accounts, which were made publicly available. This was likely from an insider attack by hactivists -- activists that use hacking as a tool.³ These figures can be corroborated from other sources, and may understate the problem. According to MicroSoft, 160 million consumer records were compromised by hacking in the first 11 months of 2015 alone.⁴

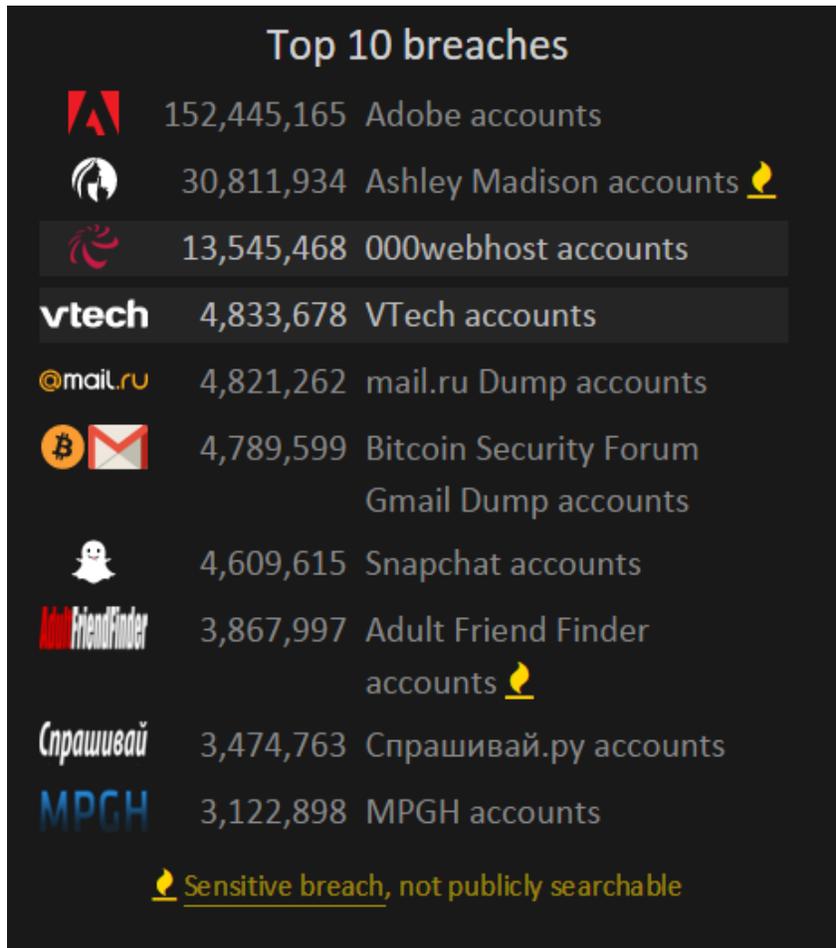


Figure 1: Hacked personally-identifiable information (PII), as of November 28, 2015.⁵

At the website haveibeenpwned.com, users can input their email address and see if their email has ever been leaked by hackers to the public. The etymology of the word “pwned” is instructive, and foreshadows three additional themes in this study. The word “owned” is often used by

² Violet Blue and Zero Day, “Find out if your data was leaked in the Adobe hack.” *ZD Net*, November 11, 2013, accessed November 30, 2015, <http://www.zdnet.com/article/find-out-if-your-data-was-leaked-in-the-adobe-hack/>.

³ Dino Grandoni, “Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions.” *The New York Times*, July 20, 2015, accessed November 30, 2015, http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?_r=0.

⁴ Keith Wagstaff, “Microsoft CEO Announces Cyber Defense Operations Center.” *NBC News*, November 17, 2015, accessed November 30, 2015, <http://www.nbcnews.com/tech/security/microsoft-ceo-announces-cyber-defense-operations-center-n464946>.

⁵ “Have i been pwned?”, accessed November 30, 2015, <https://haveibeenpwned.com>.

hackers when they obtain administrative rights to a computer network. It comes from gamers -- online video game users -- who use the term “owned” and “own” to indicate that they vanquished a foe. An example of usage is, “I beat him badly in Minecraft. I owned him.” A computer programmer in the game Warcraft once misspelled the word “own” as “pwn”, leading to millions of misspellings across millions of screens worldwide, and an inside joke among gamers to use “pwn” instead of “own”. As will become increasingly apparent in this study, gaming culture is inextricable from home-grown cyber-threats.

A virtual youth subculture of Generation Y (born after ~1980) and Generation Z (born after ~2000) exists that have different practices, ethics and mores than previous generations. These practices, ethics and mores have developed not as much from religion, philosophy, books, or mass media, as in previous generations, but from segmented and sometimes quite small and self-selected virtual communities. A subsection of Gen Y and Gen X individuals see themselves as part of an online gaming community, or even a gaming family with loyalty not only to a single game, but to a single game’s chat-room hosted by a star player.

Second, a connection exists between these virtual gaming communities, and hackers. They use the same language. They are young, desire recognition, and want a real-world outlet for their programming skills.

Third, these hackers (who are often also gamers), by virtue or non-virtue of their non-academic pursuit of virtual violence, and even the extension of that virtual violence through hacking to real-world damage, may be increasingly desensitized to real violence and may not fully understand the real-world threat that misuse of their skills has for society. They live, all too often, in a world of fantasy gaming which is difficult for them to disambiguate from real life.

This is the brave new world into which societies have been unknowingly evolving -- a world in which the top cyber-skills are held by the very young, and in which older generations are to some extent, held hostage. The cyber-security companies are all-too often playing catch-up, with the younger and more mathematically- and programming-capable minds racing ahead to find zero-day exploits worth hundreds of thousands of dollars when sold to criminals, intelligence organizations, and security companies.⁶

Cyber-security relies in the first instance on culture. Where culture breeds negativity, it will breed insecurity, whether in the cyber-realm or otherwise. Where it breeds positivity among the young, with one would hope, guidance by more mature generations, security should ensue. The still-rising level of cyber-insecurity from crime and terrorism suggests that the battle between classical ethics and youthful technical capabilities is ongoing. The jury is out as to who will win, or whether there will be a winner at all. Meanwhile, it behooves us to understand the threats.

⁶ Nicole Perloth, “In a Global Market for Hacking Talent, Argentines Stand Out.” *The New York Times*, November 30, 2015, accessed December 1, 2015, <http://www.nytimes.com/2015/12/01/technology/in-a-global-market-for-hacking-talent-argentines-stand-out.html>.

Crime

Cyber-crime is vast and likely to grow in 2016 as the proliferation of hardware, software, and apps continue apace. In 2015, a single group of cyber-criminals successfully garnered as much as \$1 billion USD in illicit proceeds -- the biggest bank heist in world history.⁷ Their high-profile lives, and occasional spectacular fails, will appeal to vulnerable individuals and aspiring criminals where barriers to entry are small -- a computer, internet connection, and programming skills.⁸

In 2015, cyber-crime hit approximately 594 million people, or 8% of the world's population. In a survey of 17 countries, Norton Cybersecurity estimated \$150 billion USD lost by consumers to cyber-crime. On average, consumers lost 21 hours each, simply in dealing with the personal impact of such crimes.⁹

But the fear of being targeted in cyber-space goes much deeper. Sixty-one percent of people feel that identity theft is more likely than ever. Approximately 80% of respondents in the Norton survey fear being a victim of online crime. Teens and children are particularly vulnerable, as they are now growing up with networked tablets in their hands, and completely innocent of the myriad online threats. Of all countries surveyed by Norton Cybersecurity, Brazilians are most worried about their teens and children falling prey to online criminals.¹⁰

United Kingdom fraud and computer misuse – incidents and number of victims				
England and Wales		Adults aged 16 and over		
Offence group	Number of incidents (000s):	Incidence Rate per 1,000 adults:	Number of victims (000s):	Victim Rate per 1,000 adults:
Fraud	5,110	112	3,757	82
Fraud with loss (including those reimbursed)	2,648	58	2,079	46
Fraud no loss	2,462	54	1,856	41
Computer misuse	2,460	54	2,113	46
Unauthorised access to personal information (including hacking)	404	9	404	9
Computer virus	2,057	45	1,741	38
Unweighted base (n= number of adults interviewed)		2,072		

1. Source: Crime Survey for England and Wales Field Trial, Office for National Statistics
 2. Field trial conducted between May and August 2015



Figure 2: Crime Survey for England and Wales Field Trial. Source: Office for National Statistics.

⁷ Owen Davis, "Hackers Steal \$1 Billion in Biggest Bank Heist in History: Could They Take Down The Whole System Next Time?" *International Business Times*, February 16, 2015, accessed November 29, 2015, <http://www.ibtimes.com/hackers-steal-1-billion-biggest-bank-heist-history-could-they-take-down-whole-system-1818010>.

⁸ Liz Moyer, "Prosecutors Announce More Charges in Hacking of JPMorgan Chase." *The New York Times*, November 10, 2015, accessed November 13, 2015, <http://www.nytimes.com/2015/11/11/business/dealbook/prosecutors-announce-more-charges-in-jpmorgan-cyberattack.html>.

⁹ "Norton Cybersecurity Insights Report." *Norton*, 2016, accessed November 21, 2015, <https://us.norton.com/cyber-security-insights>.

¹⁰ Ibid.

The absolute number of cyber-crimes is impressive, but it helps to put it in context. The United Kingdom's Office of National Statistics (ONS) used survey methodology to estimate the percentage of the population affected by cyber-crime. They report 2.5 million cases of computer misuse from June 2014 to June 2015, including 404,000 cases of hacking and identity theft.¹¹

Computer viruses infected 2.1 million computers in the United Kingdom over this period. This estimate is based on a random sample of 2,072 persons surveyed between May and August, 2015. The data, which likely understates the risk given lack of user knowledge of computer misuse, or because respondents are worried over the stigma of having a computer virus, suggests that 5.4% of the U.K. population was subject to either identity theft (.09%) or a computer virus (4.5%) during this time period. Figure 2, above, gives more detail on the UK study. This compared to over 11% subjected to some other form of fraud.¹²

The criminal threats are international, growing, and menace all networked consumers, businesses, and government. The cyber-crime group known as Carbanak, discovered in February 2015, is composed of Russian, Ukrainian, and Chinese hackers. As mentioned earlier, they completed heists of as much as \$1 billion USD from hundreds of banks internationally -- the most successful bank robbers, and the most successful cyber-criminals, in all of world history. The Carbanak gang was discovered, but it is still operating. Their malware has infected banking and financial systems around the world, and the criminals continue to use their access to transfer millions of dollars to their accounts.¹³

Other major 2015 cyber-crimes illustrate the continued robustness of this particular type of criminality. Hackers got access to as many as 14,000 social security numbers and billing accounts of the Sacred Heart Health System in March.¹⁴ An Israeli hacker named "Gabi the Georgian," made hundreds of millions of dollars from diverse forms of cyber-criminality, including from the 2014 J.P. Morgan hacks. He was arrested in July, but his accomplices are at-large.¹⁵ Hackers stole PII from 4 million customers of the London-based telecommunications group, TalkTalk. The share price dropped by almost 11% in November, implying a loss of \$900 million

¹¹ "Improving Crime Statistics in England and Wales." *Office for National Statistics*, October 15, 2015, accessed November 21, 2015, <http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html>; Crime Survey for England & Wales, *CSEW Fraud and Cyber-crime Development: Field Trial*. JN123456. (TNS January 1, 2014), accessed November 21, 2015, <http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/methodological-notes/methodological-note---csew-fraud-and-cyber-crime-development--field-trial--october-2015.pdf>.

¹² "Improving Crime Statistics in England and Wales." *Office for National Statistics*, October 15, 2015, accessed November 21, 2015, <http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html>; Crime Survey for England & Wales, *CSEW Fraud and Cyber-crime Development: Field Trial*. JN123456. (TNS January 1, 2014), accessed November 21, 2015, <http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/methodological-notes/methodological-note---csew-fraud-and-cyber-crime-development--field-trial--october-2015.pdf>.

¹³ Joseph Menn, "Cybercrime ring steals up to \$1 billion from banks: Kaspersky." *Reuters*, February 14, 2015, accessed November 30, 2015, <http://www.reuters.com/article/2015/02/15/us-cybersecurity-banks-idUSKBN0LJ02E20150215>.

¹⁴ Michael Finch II, "Sacred Heart Health System notifies 14,000 patients of data breach after hacking attack." *AL.com*, March 18, 2015, accessed November 30, 2015, http://www.al.com/business/index.ssf/2015/03/sacred_heart_health_system_not.html.

¹⁵ Orr Hirschauge and Nicole Hong, "Accused Mastermind of J.P. Morgan Hack a Product of Israel's Internet Underbelly." *The Wall Street Journal*, November 21, 2015, accessed November 21, 2015, <http://www.wsj.com/articles/accused-mastermind-of-j-p-morgan-hack-a-product-of-israels-internet-underbelly-1448101982>.

USD to the company's market capitalization. Hackmageddan.com lists scores more cyber-criminal attacks -- for each month of 2015.¹⁶

Hacktivism

Money is not the only motivator for cyber-crime; ideology and thrill-seeking inspires many hackers. Once they obtain hacking skills, they tend in later years to turn those skills towards more lucrative criminality, or ironically, to careers in cyber-security.

As mentioned above, hacktivists are hackers motivated by activist causes. Oxford Dictionaries defines a hacktivist as a "computer [hacker](#) whose activity is [aimed](#) at promoting a social or political [cause](#)."¹⁷ They are often active in hacking and then leaking data, and causing damage to targeted computer systems or accounts. The Ashley Madison leak was a form of activism -- the hackers demanded that the site come down, or they would release the email addresses of 37 million users, come what may in those users' broken personal relationships. They only released the names after Ashley Madison, self-valued at \$1 billion USD and with \$55 million USD in annual pre-tax profits, declined to shut down the website. The outing of celebrities, politicians, neighbors, and spouses had massive implications for them and their families.

The most active hacktivists, called Anonymous or Anon, emerged around 2004 on a website called 4chan.org. Anon has been described as a "shape-shifting subculture" of hackers. Members simply claim to belong -- there is no official list of members. Most are actually not hackers -- they are simply protesters. In November 2013, several thousand Anon protesters, including actor Russell Brand, marched in support of the group.¹⁸

¹⁶ Daniel Thomas and Aliya Ram, "Teenage TalkTalk cyber suspect released on bail." *Financial Times*, October 27, 2015, accessed November 30, 2015, <https://next.ft.com/content/f5c45562-7c07-11e5-98fb-5a6d4728f74e>; Madhumita Murgia, "TalkTalk Share Prices drop Almost 11pc as Metropolitan Police Investigation Continues." *The Telegraph*, October 23, 2015, accessed November 30, 2015, <http://www.telegraph.co.uk/technology/internet-security/11951797/TalkTalk-share-prices-drop-almost-11pc-as-Metropolitan-Police-investigation-continues.html>.

¹⁷ Oxford Dictionaries, "Hacktivist", accessed 12/8/2015, http://www.oxforddictionaries.com/us/definition/american_english/hacktivist.

¹⁸ Adam Withnall, "Russell Brand joins Million Mask March in London as violence breaks out between police and protesters." *Independent*, November 6, 2014, accessed November 30, 2015 <http://www.independent.co.uk/news/people/russell-brand-joins-million-mask-march-in-london-as-violence-breaks-out-between-police-and-9842970.html>.



Figure 3: A photo that promotes hacking ISIS, published on the Anon hacktivist website anonhq.com.¹⁹

Anon targets an eclectic mix of religious, state, and terrorist actors. Their ideology is probably closest to that of anarchism or vigilantism as it is anti-authoritarian, decentralized, and averse to governments, religious extremists, and ideology in general (other than their own amorphous non-ideology of individualism, anonymity and privacy). In 2014 public outcry against Anon forced them to issue an apology for doxing (research and release of PII on) a person they wrongly thought responsible for the killing of Michael Brown in Ferguson, Missouri.²⁰ In their #OpFerguson campaign, they outed a non-uniformed police dispatcher who was at his desk at the time of the shooting. He consequently received hundreds of death threats and was put under 24-hour police protection for seven days until police announced the real shooter.²¹

The invasion of privacy and slander of Anon's victim in Ferguson, without due process of law, hurt their cause immensely. But the group lives on and was as active as ever in 2015. In November following the Paris terrorist attacks, Anon claimed to have deleted 20,000 Islamic State (a.k.a. ISIS, ISIL, Daesh) Twitter accounts.²² Some Anon sources claimed the removal of 101,000 ISIS-related Twitter accounts, 5,900 propaganda videos, and 150 websites.²³ Figure 3 above shows Anon marketing on its #OpIsis campaign against the Islamic State. In late November, Anon protested Icelandic whaling through their #OpWhales campaign that took down

¹⁹ AnonWatcher, "Anonymous Takes Down 20,000 Twitter Accounts." *We Are Anonymous*, November 22, 2015, accessed November 30, 2015, <http://anonhq.com/anonymous-takes-down-20000-twitter-accounts/>.

²⁰ David Kushner, "What Anonymous Got Wrong in Ferguson." *The New Yorker*, September 5, 2014, accessed November 30, 2015, <http://www.newyorker.com/tech/elements/anonymous-got-wrong-ferguson>.

²¹ Ibid.

²² AnonWatcher, "Anonymous Takes Down 20,000 Twitter Accounts." *We Are Anonymous*, November 22, 2015, accessed November 30, 2015, <http://anonhq.com/anonymous-takes-down-20000-twitter-accounts/>.

²³ "Anonymous warned intelligence services of threatened ISIS attacks for November 22nd." *UncoverInfo*, November 21, 2015, accessed November 30, 2015, <https://undercoverinfo.wordpress.com/2015/11/21/anonymous-warned-intelligence-services-of-threatened-isis-attacks-november-22nd/>.

five websites belonging to the Government of Iceland, including those of the Prime Minister, Minister of Interior, and Minister of Environment.²⁴

This sort of vigilantism, uncontrolled by electorates or individual rights, and unaccountable because of anonymity, is a profound danger to the principles of democratic rule of law. However legitimate any particular campaign may be, and we sympathize with some of Anon's causes, the ends don't justify the means when those ends threaten the principles upon which democracy is founded.

Case Study of the Virtualization and Anomie of Youth: Twitch and Swatting

Cyber-crime can originate from hacktivism, but in what type of culture does hacking originate? What is the primordial ooze, as it were, of hackers? What is the virtual soil in which cyber-criminals incubate and hatch? As society becomes increasingly digitalized, and as we interact with the world via virtual channels, a sense of anonymity, anomie, negativity, and non-reality can creep into some young minds.

The majority of subculture websites do much good -- they are places where people with diverse interests who are geographically disparate can meet, share, and learn. This is one of the great unintended consequences of the internet. However, subculture chatrooms can also serve as cultural ghettos where extremism finds genesis. Vulnerable people return time and again to these anaerobic environments, walled off from diverse outside voices that could defend young minds from extremism.

It is in these degraded and cloistered chat rooms of subculture websites where, in at least a few instances, negativity, hacking and other forms of extremism incubate. We saw above that the hacktivist group Anon emerged from 4chan.org, a raunchy and often negative website that caters to subculture chatroom participants. The gaming website Twitch, similarly, and its connection to a practice called "Swatting" is a case study in the ethical impoverishment of youth by their new-found online "communities."

Twitch was founded in 2011, and features video-game players side-by-side with streaming live views of their online-gaming. In 2014, Amazon bought Twitch for \$1 billion USD in cash.²⁵ Viewers skyrocketed to 100 million per month. It is the fourth-largest source of U.S. internet traffic, after Netflix, Google, and Apple.²⁶ Figure 4 below shows a screenshot of one gamer on Twitch being watched by over three-thousand viewers.

²⁴ Ragnhildur Siguroardottir and Sabina Zakadzki, "Anonymous hackers target Iceland sites in whaling protest." *Reuters*, November 28, 2015, accessed November 30, 2015, <http://www.reuters.com/article/2015/11/28/us-iceland-hackers-idUSKBN0TH0GJ20151128#YAaMHx9Fud8EAloF.97>.

²⁵ Jason Fagone, "The Serial Swatter." *The New York Times*, November 24, 2015, accessed November 29, 2015, <http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html>.

²⁶ Sarah Needleman, "Twitch's Viewers Reach 100 Million a Month," *Wall Street Journal*, January 29, 2015, accessed December 8, 2015, <http://blogs.wsj.com/digits/2015/01/29/twitchs-viewers-reach-100-million-a-month/>.

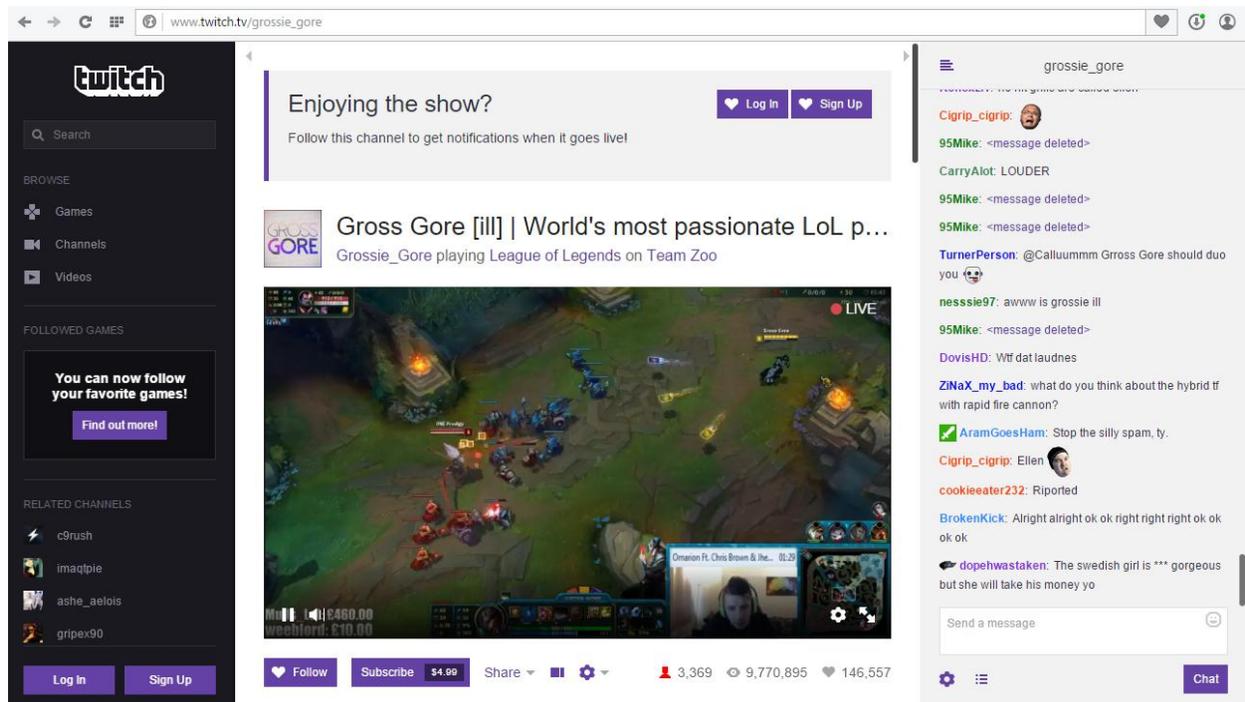


Figure 4: A screen-shot of the Twitch online gaming site.

The main photo is a live streaming video game played by “Gross Gore,” a famous video gamer with 9.8 million views. He is visible with ear-phones in the bottom-right of the game screen, and had 146,557 followers at the time of writing. Over three-thousand Twitch users were watching the game at the moment the screen-shot was taken. The average age of Twitch users is 21, and the site gets 45 million viewers per month.²⁷ On the right-side of the screen-shot is a rapidly scrolling list of obscenities and shallow commentary.

Twitch illustrates how as some youth become networked, cloistered, and involved in unsupervised subculture fantasies, including viewing and violent virtual-interaction with other fantasy gamers, they could to some extent be losing contact with a full understanding of the consequences of real-world actions. “The Internet is affecting global social behavior across the board,” according to Minds.com cofounder and CEO Bill Ottman. “Look at what Facebook is doing with virtual reality and Oculus. Talk about disconnecting from reality. People will literally start living in a proprietary digital dreamworld.”²⁸

Perhaps at least in part because of this decontextualization from reality, a new and dangerous variant of hoax has arisen, called swatting.²⁹ When someone is swatted, it means that a prank caller calls a real-world police department with a hoax emergency situation, supposedly from or near the victim’s location, but in reality likely from far away. The situation that the hoaxer recounts to the police is designed by the hoaxer to require a SWAT tactical team. The hoax must

²⁷ Mike Williams, “Twitch Viewers More Than Double to 45 Million in 2013.” *US Gamer*, January 16, 2014, accessed November 29, 2015, <http://www.usgamer.net/articles/twitch-viewers-more-than-double-to-45-million-in-2013>.

²⁸ Bill Ottman. Personal communication. December 6, 2015.

²⁹ Jason Fagone, “The Serial Swatter.” *The New York Times*, November 24, 2015, accessed November 29, 2015, <http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html>.

include the claim of an active shooter who has killed and claims to be ready to kill again, including threats to police officers. The police are then forced to respond with a team equipped with military hardware such as semi-automatic weapons, body armor, and armored tactical vehicles. As the police department does not know that the call is a hoax meant to target an innocent victim, the police assemble and dispatch the SWAT team, only to be surprised by a non-threatening situation at the hoax victim's home.

This is dangerous for the hoax victim as the SWAT team may accidentally shoot the victim, and a major cost for the police department. A SWAT team killed a former Marine and Iraq war veteran in 2011, and a 7-year-old girl in 2010, in both instances from a false alarm. Hoax swatting among online gamers, with all attendant dangers, has happened dozens of times, sometimes by the same teenager.³⁰ In one case where a gamer was confused and didn't cooperate with police orders, he was shot in the face twice with a rubber bullet and is seeking to sue the police department.³¹

The anonymous subculture websites that have risen with the rise of the internet have given proto-criminals a place to find other like-minded individuals with whom they can gain moral support in their criminal activities. While subculture websites are important to the freedom, growth, and diversity of contemporary culture, they are also at times a source of hacking and attendant criminal forms.

Terrorism

Globalization and the internet age provide the world with new possibilities and efficiency, empower citizens and regularize widespread access to information. However, these forces can also be utilized as tools for unregulated cyber terror -- a terrorism without borders and with no theoretical limits. This study argues that the threat of cyber-terror will be a cause for increasing concern in 2016. We discuss the biggest cyber-terror threats, including from Islamic State, Al-Qaeda, and Boko Haram; cyber-terror tactics, including potential takeover of command and control of industrial and military systems; and the devastating effects such terrorist control could wreak.

In a world where Islamic State is threatening to set up a cyber caliphate,³² and where terrorist groups' websites can "serve as virtual training grounds," by offering tutorials on firing surface-to-air missiles, building bombs, shooting at U.S. soldiers, and how to enter Iraq from abroad,³³ the internet forms not only a place for propaganda or a way to project power without borders, but also a terrifying weapon that can be used for terrorist takeover of financial systems, dangerous industrial processes, and strategic weapons systems.

³⁰ Ibid.

³¹ Liz Klimas, "'Swatting' Prank Ends Horribly for Victim - and He Has the Injury to Prove It." *The Blaze*, July 16, 2015, accessed November 29, 2015, <http://www.theblaze.com/stories/2015/07/16/swatting-prank-ends-horribly-for-victim-and-he-has-the-injury-to-prove-it/>.

³² Jamie Dettmer, "Digital Jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US," *Fox News*, September 14, 2014, accessed September 18, 2015, <http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/>.

³³ Eben Kaplan, "Terrorists and the Internet," *Council on Foreign Relations*, January 8, 2009, accessed September 18, 2015 <http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005>.

Cyber-terrorists operate in a Wild West of unregulated and international virtual spaces. Expert Gabriel Weimann explains, “The rise of the global jihad movement in the recent decades has coincided with the expansion and development of online communication platforms.”³⁴ He goes on to explain that these anonymous platforms are ideal for terrorists as they are decentralized, outside the scope of restriction, without censorship, and openly accessible to whoever wants them,³⁵ all while bypassing “traditional channels of authority”³⁶ and empowering non-state actors as a result.

With the “internet as the poster child of globalization,”³⁷ terrorist organizations have had a significant and evident interest in improving and using cyber capabilities to forward their causes.³⁸ One must look no further than online recruitment tactics employed by Islamic State³⁹ and Boko Haram using social media, or the 1,400 names, email addresses, and passwords of U.S. military personnel and government employees the Islamic State Hacking Division published in 2015 with the message “Oh Crusaders... know that we are in your emails and computer systems, watching and recording your every move...”⁴⁰ Though cyber-terrorism follows predecessors in garnering new technology to act upon strategic vulnerabilities,⁴¹ this tool knows no borders and provides the smart terrorist with perfect anonymity. Unlike in the case of a nuclear threat during the Cold War, deterrence plays no, or almost no, mitigating role.

Definition of Cyber-Terrorism

First, it is crucial to define ‘cyber-terrorism’ as a concept. As the Federal Bureau of Investigation (FBI) says, cyber-terrorists are different from other cyber threats such as hackers, hackers for hire, and global cyber syndicates.⁴² More specifically, the FBI defines cyber-terrorism as “premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents.”⁴³

³⁴ Gabriel Weimann, “Cyber-Fatwas and Terrorism,” *Studies in Conflict & Terrorism* 34 (2011): 769.

³⁵ Ibid. 769.

³⁶ Ibid. 779.

³⁷ Lee Jarvis, Lella Nouri and Andrew Whiting, “Understanding, Locating and Constructing Cyberterrorism,” in *Cyberterrorism: Understanding Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis and Stuart Keith Macdonald (New York: Springer, 2014), 25.

³⁸ Tope Aladenusi, “‘Cyberharam’: can Nigeria prepare for the next generation of terrorists?” *Deloitte Insights*, June 2014, accessed September 20, 2015, <http://www2.deloitte.com/ng/en/pages/risk/articles/cyberharam-can-nigeria-prepare-for-the-next-generation-of-terrorists.html>.

³⁹ Ibid.

⁴⁰ Dugald McConnell and Brian Todd, “Purported ISIS militants post list of 1,400 U.S. ‘targets’,” *CNN*, August 13, 2015, accessed September 20, 2015, <http://www.cnn.com/2015/08/13/world/isis-militants-american-targets/index.html>.

⁴¹ James A. Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,” *Center for Strategic & International Studies*, December 2002, accessed September 20, 2015, <http://www.stepto.com/publications/231a.pdf>.

⁴² Robert Anderson Jr., Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, September 10, 2014, Washington, DC.

⁴³ Peter W. Singer, “The Cyber Terror Bogeyman,” The Brookings Institution, November 2012, accessed September 20, 2015, <http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer>.

The FBI definition is unfortunately too restrictive, in that it does not include, for example, other cyber-techniques like cyber-espionage and cyber-crime that are used in service of traditional terrorist tactics and groups. It is over-broad in that it includes clandestine agents, which are often state-backed. Finally, it does not include failed cyber-terrorism that does not result in violence. But we know that a failed terrorist is still a terrorist, and therefore a failed cyber-terrorist must still be a cyber-terrorist.

We therefore propose a new definition. *Cyber-terrorism is the use of cyber methods by non-state actors either to: cause terror, including through intended serious physical harm to, or infiltration of, persons, property, or networks; or, act in support of traditional terrorism.*

Cyber-terrorism is not conducted by governments, such as for example the Chinese hackers in June 2007,⁴⁴ nor is it limited to prominent online terrorists such as Irhaby 007 and Abu Maysarah al-Iraqi.⁴⁵ Rather, cyber-terrorism is committed by non-state actors who are often completely unknown.

Terror Groups that use Cyber Tactics

This section will focus on cyber tactics utilized by three of the world's most dangerous terrorist organizations: Islamic State, Al-Qaeda, and Boko Haram.

Such tactics are particularly conducive to non-state actors and terrorist organizations (as well as small states), because as with cyber-crime, the low barriers to entry in cyberspace enable even the smallest terrorist organizations to have a large impact.⁴⁶ As Steve Stalinsky, Executive Director of The Middle East Media Research Institute explains:

The jihadists are investing a lot in encryption technologies and they have developed their own software to protect their communications and when Western agencies work out how to crack them they adapt quickly.... They are forward-thinking and are experimenting with hacking. In the future, the jihadist cyber army's activities will become a daily reality.⁴⁷

Islamic State

Islamic State (also known as ISIS, ISIL, IS, Daesh) is a non-state terrorist organization that became internationally known in 2014 after seizing large swathes of land in Syria and Iraq. It has a mission to establish a regional (but potentially global) caliphate governed in accordance with Sharia law. ISIS calls for all Muslims to swear allegiance and migrate to areas under Islamic

⁴⁴ Eben Kaplan, "Terrorists and the Internet," *Council on Foreign Relations*, January 8, 2009, accessed September 18, 2015, <http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005>.

⁴⁵ Ibid.

⁴⁶ Nye, "From bombs to bytes: Can our nuclear history inform our cyber future?" 9.

⁴⁷ Jamie Dettmer, "Digital Jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US," *Fox News*, September 14, 2014, accessed September 18, 2015, <http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/>.

State control.⁴⁸ ISIS also commonly uses brutal tactics, including but not limited to abduction, rape, enslavement, beheading and mass killings.⁴⁹ Remarkably, Islamic State methods make Al Qaeda and the Taliban look moderate in comparison.

Islamic State has used its barbaric techniques as propaganda broadcasted over social media channels.⁵⁰ It is also known for its use of the internet as an international recruitment tool⁵¹ and for inspiring, radicalizing and coordinating with affiliates in other countries to carry out attacks, such as Paris in November 2015.⁵² Its ability to harness social media to gain attention, recruits, and radicalize affiliates can be considered one of the group's most serious threats.

The Islamic State has threatened to set up a "cyber caliphate" to conduct massive cyber attacks on Western countries' financial and infrastructure systems.⁵³ These efforts are ascribed to Abu Hussain Al Britani, a known ISIS hacker and fighter killed in a United States airstrike in early 2015. Abu Hussain, before being killed, called for "computer-literate jihadists to come to Syria and Iraq" to further the cyber-caliphate.⁵⁴

Furthermore, the FBI has warned of these possible cyber threats, specifically those aimed at U.S. networks and critical infrastructure by Islamic hacktivists affiliated with or in support of ISIS' *cyber-call-to-action*.⁵⁵ For example, the 'IS hacking division,' as mentioned earlier, published 1,400 names, email addresses, passwords and other PII of government employees and military personnel with claims to "strike at your necks in your own lands!"⁵⁶ This is the second time this year that a group claiming to be part of ISIS has acted similarly.⁵⁷

The warnings about ISIS' cyber-attacks are becoming more common. According to George Osborne, the United Kingdom's Chancellor of the Exchequer, ISIS is trying to build its capability to use cyber-attacks on infrastructure (hospitals and air traffic control systems) to kill large numbers of people.⁵⁸ The Director of the FBI, James Comey, also warned that ISIS was

⁴⁸ "What is 'Islamic State'?" *BBC*, June 29, 2015, accessed Sept. 20, 2015, <http://www.bbc.com/news/world-middle-east-29052144>.

⁴⁹ *Ibid.*

⁵⁰ "How ISIS Began Using Beheadings As Propaganda." *NBC News*, March 10, 2015, accessed December 1, 2015, <http://www.nbcnews.com/video/gunman-ambushes-firefighters-577304643682>.

⁵¹ Aladenusi, "Cyberharam': can Nigeria prepare for the next generation of terrorists?"

⁵² Paul Tassi, "How ISIS Terrorists May Have Used PlayStation 4 to Discuss and Plan Attacks." *Forbes*, November 14, 2015, accessed December 1, 2015, <http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/>.

⁵³ Jamie Dettmer, "Digital Jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US," *Fox News*, September 14, 2014, accessed September 18, 2015, <http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/>.

⁵⁴ *Ibid.*

⁵⁵ Marcos Colón, "FBI warns of potential cyber attacks launched by ISIS hacktivists," *SC Magazine*, September 29, 2014, accessed September 20, 2015, <http://www.scmagazine.com/fbi-warns-of-isis-hackivist-cyber-attacks-on-us/article/374283/>.

⁵⁶ Dugald McConnell and Brian Todd, "Purported ISIS militants post list of 1,400 U.S. 'targets.'"

⁵⁷ *Ibid.*

⁵⁸ Dan Bloom, "ISIS trying to launch deadly cyber-attack on airports, hospitals and National Grid warns George Osborne." *The Mirror*, November 17, 2015, accessed December 1, 2015, <http://www.mirror.co.uk/news/uk-news/isis-trying-launch-deadly-cyber-6845517>.

exploring the possibility of “using sophisticated malware to cyberattack critical infrastructure in the U.S.”⁵⁹

In fact, the Department of Homeland Security’s Assistant Secretary for Infrastructure Protection, Caitlin Durkovich, confirmed in October 2015 that ISIS had begun “to perpetrate cyberattacks” but had thus far been unsuccessful. Currently, ISIS cyber capabilities are weak due to their use of unsophisticated hacking tools. According to the FBI’s Cyber Division Section Chief John Riggi, “the concern is that they’ll buy that [more sophisticated] capability” on the black market.⁶⁰

As Islamic State is increasingly driven underground by coordinated (and sometimes not-so-coordinated) airstrikes from the United States, Russia, Syria, Turkey, France, Britain, and others, we can expect their cyber-caliphate to gain more prominence and budgetary priority. Islamic State’s fighters will increasingly resort to cyber-tactics in 2016, along with other more traditional subversive tools such as improvised explosive devices (IEDs) and terrorist attacks in Europe and the United States.

Al-Qaeda

Al-Qaeda is a transnational movement and terrorist network founded in 1988. The group is infamous for its attack on New York City’s World Trade Center in 2001 and the Madrid bombings in 2004. Since 2001, their use of the internet as a tool has increased significantly.⁶¹ Al-Qaeda has been known to use technology for propaganda, such as the attention received through the posting of videos,⁶² and as a tool for intra-group communications, fundraising and public relations.⁶³

Additionally, Omar Bakri Muhammad has claimed that there are “tens of thousands of bin Laden supporters who are studying computer science in order to work for the holy cause.”⁶⁴ Al Qaeda has websites with tactical information on how to design bomb belts,⁶⁵ and information technology sections where knowledge for electronic jihad is shared.⁶⁶

Under the umbrella of Al-Qaeda since its merge in 2012, Al-Shabaab’s internet usage has grown exponentially. This technological use has had the effect of expanding Al Shabaab’s reach from

⁵⁹ Wesley Bruer, “FBI chief worries ISIS could use cyberattacks against U.S.” *CNN*, May 21, 2015, accessed December 1, 2015, <http://www.cnn.com/2015/05/20/politics/isis-cyberattack-fbi-director/>.

⁶⁰ “ISIS is attacking the U.S. energy grid (and failing).” *CNN Money*, October 16, 2015, accessed December 1, 2015, <http://money.cnn.com/2015/10/15/technology/isis-energy-grid/>.

⁶¹ Heickero, “Cyber Terrorism: Electronic Jihad,” 557.

⁶² Eben Kaplan, “Terrorists and the Internet,” *Council on Foreign Relations*, January 8, 2009, accessed September 18, 2015, <http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005>.

⁶³ Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.”

⁶⁴ Heickero, “Cyber Terrorism: Electronic Jihad,” 558.

⁶⁵ *Ibid.*, 560.

⁶⁶ *Ibid.*, 561.

being largely confined in Somalia, to being a global threat. They are exploiting the internet to recruit followers, source funding and spread propaganda for their operations.⁶⁷

Such activities, both by Al-Qaeda and Al-Shabaab, are expected to continue in 2016. Whether or not they expand this activity will have more to do with these groups' relative power with respect to ISIS and other rapidly expanding extremist groups, as ISIS was actively challenging Al Qaeda affiliates in 2015 through superior outreach, recruiting, and targeting.⁶⁸

While the group size of Al Qaeda and ISIS may be negatively correlated, because they are adversaries in the fields of recruiting and battle, the number of cyber-terrorist individuals is independent of the relative strength between Al Qaeda and ISIS. Whichever group they fight for in cyberspace, they fight nonetheless, and the tactics and reach of cyber-terrorists are growing.

Boko Haram

Boko Haram, another militant Islamist group, has also used cyber tactics. Founded in 2002, Boko Haram was designated a terrorist group by the United States in 2013. It is based in Nigeria and has induced a wave of bombings, assassinations and abductions to overthrow the government and create an Islamic state.⁶⁹ Boko Haram also harnesses social media to garner attention for its cause and new recruits.⁷⁰

As an example of its cyber-terrorist tactics, in 2013 Boko Haram hacked databases of personnel records, revealing names of Nigeria's secret service, including addresses and bank information.⁷¹ Boko Haram also used over 400 letter frauds and other scams to generate funding in four months since pledging its allegiance to ISIS in January 2015. Its propaganda videos and social media presence have improved since aligning with ISIS.⁷² Nigerian companies have also been victims of cyber-attacks, including NAIJ.com, a news and entertainment website in Nigeria attacked in July 2015, and Premium Times attacked during the elections in 2015. The perpetrators are unknown, but Boko Haram is suspected by analysts.⁷³

The involvement of these three groups: Al Qaeda, Islamic State, and Boko Haram in cyber attacks and cyber-terrorism as described in the above examples serves as clear evidence that

⁶⁷ Peter Kagwanja and Moses Karanja, "How cyber-crime complicates war on terror," *The East African*, August 10, 2014, accessed September 20, 2015, <http://www.theeastafrican.co.ke/news/How-cyber-crime-complicates-war-on-terror/-/2558/2422854/-/h5krwj/-/index.html>.

⁶⁸ Gregory D. Johnsen, "This man is the leader in ISIS's recruiting war against Al-Qaeda in Yemen," July 6, 2015, accessed 12/2/2015, <http://www.buzzfeed.com/gregorydjohnsen/this-man-is-the-leader-in-isis-recruiting-war-against-al-qaе>.

⁶⁹ Farouk Chothia, "Who are Nigeria's Boko Haram Islamists?" *BBC*, May 4, 2015, accessed September 20, 2015, <http://www.bbc.com/news/world-africa-13809501>.

⁷⁰ Aladenusi, "Cyberharam: can Nigeria prepare for the next generation of terrorists?"

⁷¹ Ioannis Mantzikos, "Exploring Nigeria's Vulnerability in Cyber Warfare," *Modern Diplomacy*, July 22, 2013, accessed September 20, 2015, http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=221:exploring-nigeria%E2%80%99s-vulnerability-in-cyber-warfare&Itemid=487.

⁷² "Terror Goes Cyber: Capabilities of Boko Haram." *Bat Blue*, April 29, 2015, accessed December 1, 2015, <http://www.batblue.com/terror-goes-cyber-capabilities-of-boko-haram/>.

⁷³ Clement Ejiofor, "From Cyber Attacks On Naij.com to Cyber Terrorism." *August 2015*, accessed December 1, 2015, <https://www.naij.com/490654-from-cyber-attacks-on-naij-com-to-cyber-terrorism.html>.

cyber-terrorism as earlier defined represents a real and growing threat. The possibility cannot be ruled out that a terrorist group could at some point hack into an industrial control system (ICS), and cause serious damage not only to the equipment that is thereby owned by the terrorists, but also through that equipment that could be used as a terrorist weapon. It is possible that terrorists could, for example, take control of a chlorine factory, nuclear missile, nuclear power plant, or algorithmic trading platform at one of the world's largest asset management companies. They could close stock exchanges or the electric grid. Any of the above would cause chaos, terror, and immense damage to Western countries and the global financial system. While the probability of such an event may be extremely low on an annual basis, it is higher when thinking by the decade. And when considering the resulting damage, the risk, or probability multiplied by cost, is quite high.

State Cyber-Tactics: Militarization, Espionage and Censorship

While cyber-criminals, thrill-seekers, terrorists, and hacktivists will continue to be the most frequent form of cyber-threat in 2016, and arguably the most dangerous, state-use of cyber tactics in militarized disputes and espionage is also a great, and also possibly the greatest, danger. As with potential terrorist takeovers of industrial control systems, states are growing their abilities in this and other areas, such as the ability to disable the internet and networked defense systems of an adversary.

The West is woefully unprepared for defense against state use of cyber tactics. The U.S. State Department Inspector General has heavily criticized the State Department every year from 2011 to 2015 for its lack of cyber-security. For example, the Chief Information Officer (CIO) in the State Department has no power to enforce cyber-security standards.⁷⁴

Foreign government and commercial entities focus on economic espionage for commercial benefit above all other forms of espionage. Wealthy nations have the most to lose from commercial espionage, as their proprietary technology assets are greater than those of developing nations. Developing nations, on the other hand, have the inexpensive labor to launch pervasive cyber-espionage operations. It is not surprising, then, that wealthy nations are the most vociferous in their statements against cyber economic espionage.

The G20 nations made a statement against cyber economic espionage in November 2015, setting up a supposedly unified front for further diplomatic initiatives in 2016.⁷⁵ However, some of the G20 nations, including China, Brazil, France, Russia, and South Africa, are known to liberally use cyber economic espionage. Despite recent statements to the contrary, we believe it unlikely that these countries will make significant strides against enforcing counter-espionage in their

⁷⁴ The Associated Press, "Audit: State Department Cyber Security Still Not Up to Par." *The New York Times*, November 20, 2015, accessed November 22, 2015, <http://www.nytimes.com/aponline/2015/11/20/us/politics/ap-us-state-department-cyber-audit.html>.

⁷⁵ Ellen Nakashima, "World's richest nations agree hacking for commercial benefit is off-limits." *The Washington Post*, November 16, 2015, accessed November 30, 2015, https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

countries, as that espionage at least holds the prospect of significantly increasing their economic growth.

This is a serious issue for companies in Western regions that must: 1) develop new technologies for the market; 2) defend against overseas competitors who carry out industrial espionage, often with their state's knowledge; and 3) compete against their own innovations when they are mass produced with inexpensive foreign labor. In addition, these same Western companies may be competing for market share against foreign companies that have a liberal approach towards corruption -- of which cyber-espionage is just one form.

It is no secret that many countries block technology and social media companies such as Google, Facebook, Twitter, and Youtube. In its annual report, "Freedom on the Net 2015," Freedom House ranked countries by their use of censorship on the internet and criminalization of certain aspects of free speech on the web. China was ranked as least-free, as detailed below.

However, China is not the only country whose government uses censorship to prevent its citizens from accessing information. According to Twitter's transparency report for the second half of 2014, Turkey makes the most requests for removing content of any country. In April 2015, Turkey blocked access to Youtube and certain social media websites including Twitter, after some users posted pictures of far-left militants of the DHKP-C holding an Istanbul prosecutor hostage. Once Twitter, Youtube, and Facebook complied with the court order to remove the image, they were unblocked.⁷⁶ This was the second ban for these types of sites in 13 months. The government previously blocked them in March 2014 right before planned local elections. The government sought to prevent the spread of recordings that purportedly had evidence of corruption by then-prime minister Recep Tayyip Erdogan's inner-circle.⁷⁷

In China, Turkey, and other authoritarian or proto-authoritarian regimes, we can expect to see continued censorship on the internet. Some of the most dangerous proposals in this trend are those that seek to balkanize or splinter the internet within national borders, such that each country has control over the influx and efflux of information.

The core of the internet – physical lines of communication – could be nationalized and bottle-necks could be emplaced to disallow outside influence. The world wide web not only could, but is being controlled by different authoritarian countries, which can easily disallow websites that, for example, could be used for social mobilization (like Twitter and Facebook), or for the spread of free information (like Google or Amnesty International). Finally, apps can and are outlawed from certain countries. The app Secret, for example, was banned in Brazil because it allows anonymous postings about individuals.⁷⁸ While this is a laudable attempt to discourage slander, it at the same time sets a dangerous precedent against freedom of speech.

⁷⁶ Raziye Akkoc, "Turkey blocks access to social media and Youtube over hostage photos." *The Telegraph*, April 6, 2015, accessed December 1, 2015, <http://www.telegraph.co.uk/news/worldnews/europe/turkey/11518004/Turkey-blocks-access-to-Facebook-Twitter-and-YouTube.html>.

⁷⁷ Ibid.

⁷⁸ Joshua Bleiberg and Darrell M. West, "How to stop the internet from breaking apart," October 6, 2014, accessed 12/2/2015, <http://www.brookings.edu/blogs/techtank/posts/2014/10/6-preventing-internet-balkanization>; Jon Russell, "Apple removes Secret from the App Store in Brazil because it breaches local free speech law," August 22, 2014, accessed 12/2/2015, <http://thenextweb.com/apps/2014/08/22/apple-removes-secret-app-store-brazil-breaches-local-free-speech-law/>.

High-Threat Countries

In this section we cover the nature of state-led and state-allowed cyber-threats from those countries most likely to commit cyber-attacks, crimes, and espionage in 2016. The defense bill passed by U.S. lawmakers in November 2015 specifically directs U.S. Cyber-command to wargame attacks from China, Russia, North Korea, and Iran.⁷⁹ The threats emanating from this group of countries is primarily state-sponsored. They see themselves as in opposition to the West, and especially the United States. They therefore seek to increase their offensive cyber capabilities, and use these capabilities liberally against the West.

We add to this list of high-risk countries from a national security perspective, several countries that we expect in the professional community to be major continued sources of cyber-crime in 2016: Brazil, India, South Africa, and Argentina. The criminal threats emanating from this latter group are a function of: 1) lack of a high-quality job supply, and 2) a highly educated and technical workforce, compared with other countries in their GDP per capita bracket. With cyber-skills but lack of sufficient job supply, a significant proportion of applicants turn to hacking and other cyber-crime.

China

Starting in 2013, a high-level Chinese hacking group known as Iron Tiger stole trillions of bytes from the U.S. government, defense contractors and other related companies. This confidential data included intellectual property, emails, and strategic planning documents. Forensic information detected on U.S. government VPN servers strongly suggests that Iron Tiger resides in China.⁸⁰ While President Xi Jinping of China promised on September 25, 2015 to halt cyberattacks on commercial and government systems -- going so far as to call them "criminal", such attacks have continued into late 2015.⁸¹

China sponsored a massive attack on the U.S. Office of Personnel Management (OPM) that started in 2014 and was not discovered until 2015. The hacks stole 5.6 million security clearance applicant fingerprints, which when tallied with the number of social security numbers and addresses, results in over 21 million people affected.⁸² As the data is on cleared government employees, and could be cross-referenced with U.S. government officials not on the list, a

⁷⁹ David E. Sanger and Nicole Perloth, "Iranian Hackers Attack State Dept. via Social Media Accounts." *The New York Times*, November 24, 2015, accessed November 30, 2015, <http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html>.

⁸⁰ Lisa Brownlee, "China-based Cyber Attacks on US Military Are 'Advanced, Persistent And Ongoing': Report." *Forbes*, September 17, 2015, accessed December 1, 2015, <http://www.forbes.com/sites/lisabrownlee/2015/09/17/chinese-cyber-attacks-on-us-military-interests-confirmed-as-advanced-persistent-and-ongoing/>.

⁸¹ Editorial Board, "Will China Keep its Cyber Promises?" *The Washington Post*, October 21, 2015, accessed November 30, 2015, https://www.washingtonpost.com/opinions/will-china-keep-its-cyber-promises/2015/10/21/c0c8e422-7775-11e5-a958-d889faf561dc_story.html.

⁸² Andrea Peterson, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought." *The Washington Post*, September 23, 2015, accessed December 1, 2015, <https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/>.

number of CIA officers purportedly were pulled from China as a precautionary measure.⁸³ The data included highly personal PII on families, illnesses, and criminal offenses of security clearance applicants. Revelations required as part of the security clearance process could be misused by the Chinese for blackmail in the future.

Unit 78020 of the People's Liberation Army has extensively hacked allies of the United States in the South China Sea. In response to Chinese hacking, in 2014 the U.S. government indicted five People's Liberation Army (PLA) officers for hacking U.S. industrial interests, including the Service Workers International Union, Westinghouse Electric Company, and Alcoa.⁸⁴

The 2015 Freedom House Report ranked China as the most censored country out of the 65 surveyed, followed by countries such as Cuba, Iran and Myanmar.⁸⁵ Through a recent criminal law, people convicted "of creating and spreading 'false information' online" could receive prison sentences of seven years. China has also drafted a new cybersecurity law that would allow the government to shut down the Internet over large regions of China, as it did to the Xinjiang region during the Uighur riots in 2009. These efforts help China prevent the spread of political dissent.⁸⁶ While slander and misinformation on the internet is dangerous to individuals and communities, laws against these infractions must be weighed against the possibly greater harm of chilling freedom of speech.

Russia

Russia is one of the worst offenders in cyber-space. The Russian Federation has been engaged in cyber-war since at least 2008. The Dukes (a cyber-espionage group) have been "working for the Russian government since at least 2008 to collect intelligence in support of foreign and security policy decision-making," according to analysts at F-Secure.⁸⁷ Russian hackers are incredibly skilled -- they are reputed to have broken into President Obama's email, as well as unclassified U.S. State Department servers.⁸⁸

Russia threatens not only U.S. data through hacking, but the physical infrastructure of the U.S. internet trunk lines. Fears among analysts are multiplying over a potential Russian cyber attack, comprising a cable cutting attack, which would severely deplete Western governments' ability for instant communications. As recently as late October of this year, Russian submarines and spy ships operated perilously close to "vital undersea cables that carry almost all global Internet

⁸³ Ellen Nakashima and Adam Goldman, "CIA pulled officers from Beijing after breach of federal personnel records." *The Washington Post*, September 29, 2015, accessed December 1, 2015, https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html.

⁸⁴ Scott Cendrowski, "Evidence of China's state-supported hacking grows." *Fortune*, September 24, 2015, accessed December 1, 2015, <http://fortune.com/2015/09/24/evidence-of-chinas-state-supported-hacking-grows/>.

⁸⁵ Edward Wong, "China Ranks Last of 65 Nations in Internet Freedom." *The New York Times*, October 29, 2014, accessed December 1, 2015, <http://www.nytimes.com/2015/10/30/world/asia/freedom-house-report-china-internet-freedom.html?ref=topics>.

⁸⁶ Ibid.

⁸⁷ F-Secure, *The Dukes: 7 Years of Russian Cyberespionage*. Whitepaper. Accessed December 1, 2015, https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf.

⁸⁸ Ibid.

communications.”⁸⁹ This, along with Russia’s other aggressive actions since 2012, have contributed to an increase in fears of a return to a Cold War footing.

Ukraine has completely insufficient cyber capabilities to defend against Russia. CyberBerkut, a hacker group claiming to come from Ukraine, is suspected to be sponsored by Russia, and launched debilitating attacks on the cyber-infrastructure of the May 2014 elections. According to Ukraine’s head of counterintelligence, Russian cyber elements are at the time of writing in 2015 seeking to infiltrate a classified Ukrainian network headquartered at Kramatorsk. Ukraine has requested cyber-assistance from NATO, which stated an intention to provide Ukraine with a cyber command center. But legislative and bureaucratic delay, as well as outright resistance in some member countries, have beguiled the project.⁹⁰

As Russia continues to push the boundaries against NATO in Eastern Europe, the Balkans, Syria, Iraq, Turkey, and with air and naval transits near European coastlines, including Sweden and the United Kingdom, we expect increased NATO-Russian conflict in 2016. With this conflict will come robust Russian cyber-operations that continue or increase the magnitude of exfiltration and sabre-rattling attacks, compared to the past few years.

Iran

As Iran is expected to ramp down its nuclear program in 2016, it is looking for other forms of weapon, and other tools of influence, powerful enough to wield on a global stage. Nuclear negotiations between the United States and Iran in 2015 saw an unprecedented increase in Iranian state use of cyber-espionage, including hacking into State Department officials’ private emails and social media.⁹¹ Iran likely knew that State Department officials have in the past illegally used private email for government, and even classified, business (e.g., Hillary Clinton).⁹²

Iran will increase its global market integration in 2016, and with it, the opportunities to garner industrial information through cyber-espionage. It will also likely continue its proxy war in Iraq and Syria, and its adversarial stance towards Israel. It’s counterparts in these conflicts, including Saudi Arabia, the United States (to some extent), and Israel, will likely be targeted through increased cyber-tactics, as will the Islamic State and Sunni militias fighting Assad.

North Korea

North Korea has been named as the culprit of a massive attack on Sony Pictures in November 2014 that released thousands of documents, including emails, personal data of employees,

⁸⁹ David E. Sanger and Eric Schmitt, “Russian Ships Near Data Cables Are Too Close to U.S. Comfort.” *The New York Times*, October 25, 2015, accessed November 16, 2015, http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0.

⁹⁰ Margaret Coker and Paul Sonne, “Ukraine: Cyberwar’s Hottest Front.” *The Wall Street Journal*, November 9, 2015, accessed November 22, 2015, <http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671>.

⁹¹ David E. Sanger and Nicole Perlroth, “Iranian Hackers Attack State Dept. via Social Media Accounts.” *The New York Times*, November 24, 2015, accessed November 30, 2015, <http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html>.

⁹² Kimberly A. Strassel, “A Clinton Email Scandal Checklist.” *The Wall Street Journal*, October 1, 2015, accessed November 30, 2015, <http://www.wsj.com/articles/a-clinton-email-scandal-checklist-1443739607>.

executive pay, and films and scripts that had not yet been released. The attack was supposedly in response to the studio's release of the film *The Interview*, which poked fun at the country. Although North Korea denies conducting the attack and others have refuted the claims, the FBI announced that it had evidence North Korea was indeed behind the attack because there were instances where the hackers were sloppy, allowing the FBI to see the IPs being used.⁹³

North Korea is also believed to be behind numerous cyberattacks on South Korea, including on banks, firms that control South Korean nuclear power plants, and television stations.⁹⁴ North Korea's cyber-attacks are likely to continue in 2016, as they can gain media attention and critical information, with a lesser risk of military confrontation.

Brazil

Brazil is considered the world's leader in online banking fraud. As one of the earliest countries to adopt online banking, it created a great opportunity for online theft on both the national and international levels. One scheme that targeted the *boleto* system of printing a bar code on a piece of paper to make a payment in Brazil (a method designed to prevent online fraud) created malware that rewrote the bar codes to reroute monetary transfers to unintended recipients, netting the hackers up to \$3.75 billion.⁹⁵

Hacking in Brazil has become a common business, as there are high financial rewards and a low probability of capture and prosecution. Brazilian cybercrime laws are considered inefficient and ineffective, and only impose light penalties. As of June 2015 Brazil had still not enacted any laws to protect personal information, which allows hackers to sell it to legal or illegal businesses without repercussion. In addition, both the federal and state cybercrime divisions lack the necessary funding and staff to be truly effective.⁹⁶

Brazil's continuing close connection with China and Russia, and lack of good rule of law, means that it will likely continue to be a location from which hacking originates in 2016.

India and Pakistan

Indian and Pakistani hackers have taken their countries' animosity into the cyber sphere. Hackers on each side deface the websites of companies, organizations, and celebrities in the other. In Pakistan this has included the railways website, electric power companies, and

⁹³ Oliver Laughland, "FBI director stands by claim that North Korea was source of Sony cyber-attack." *The Guardian*, January 7, 2015, accessed December 1, 2015, <http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey>.

⁹⁴ Anna Fifield, "Seoul seeks hacker troops to fend off North Korean cyberattacks." *The Washington Post*, October 25, 2015, accessed December 1, 2015, https://www.washingtonpost.com/world/asia_pacific/south-korea-seeks-hackers-to-defend-against-north-korean-cyberattacks/2015/10/24/88bcba0-7682-11e5-a5e2-40d6b2ad18dd_story.html.

⁹⁵ Lourdes Garcia-Navarro, "Brazil's Cybercrime Free-For-All: Many Scams and Little Punishment." *National Public Radio*, June 16, 2015, accessed December 1, 2015, <http://www.npr.org/sections/parallels/2015/06/15/414622197/brazils-cybercrime-free-for-all-many-scams-and-little-punishment>; accessed 12/2/2015, <http://www.nytimes.com/2014/07/03/technology/cybercrime-scheme-aims-at-payments-in-brazil.html>.

⁹⁶ Ibid.

Pakistan People's Party (PPP), the main opposition party.⁹⁷ Pakistani hackers, for their part, crashed the Indian state of Kerala website and posted a picture of a burning Indian flag. In response, Indian hackers crashed a number of Pakistani government websites, including those of the Pakistani President and Cabinet.⁹⁸

Interestingly, this might suggest that interstate relations are immune, on at least a military response level, to these unfortunate state-level pranks. Cyber-disputes such as this are likely to continue between India and Pakistan, as well as other countries and entities which are not in an outright military conflict. The key for policy leaders is to ensure that these cyber-pranks do not escalate to higher levels of militarized dispute.

Developing Countries

Argentine hackers have a reputation for being some of the best and most creative hackers in the world. Credited to a culture of breaking rules and circumventing law due to decades of military dictatorship and ongoing strict import regulations that affect many modern technologies, the Argentinians are known for being particularly skilled in finding zero-day flaws. Selling zero-day exploits is a lucrative business, as Apple's payout of \$1 million for an exploit last October demonstrates.⁹⁹ Foreign governments and companies recruit hackers by attending hacking conferences such as EkoParty, the largest of its kind in Latin America. At this annual event hackers demonstrate their skills to a large swath of interested parties, from Silicon Valley start-ups to well-established consulting firms.¹⁰⁰

Hacking is a growth industry in Argentina, and will likely remain so in 2016. Wages are comparatively low, and the population is highly educated. Hacking provides an avenue to either established security work, or if that fails, criminal careers.

In some respects similarly to Argentina, developing country internet and security infrastructure more generally is particularly vulnerable as a lack of cyber-security personnel, out-dated hardware, and pirated software (without automatic updating) makes consumer, commercial, and government online activity accessible to hackers. This is especially the case in Africa, where most citizens are still off-line, using mobile phone technology and internet cafes, rather than smart phones and home broadband networks.

⁹⁷ Kim Arora, "Hackers from India, Pakistan in full-blown online war." *The Times of India*, October 10, 2014, accessed December 1, 2015, <http://timesofindia.indiatimes.com/tech/tech-news/Hackers-from-India-Pakistan-in-full-blown-online-war/articleshow/44766898.cms>.

⁹⁸ Sachin Jose, "Mallu Cyber Soldiers' retaliates by hacking Pakistan government websites." *International Business Times*, September 27, 2015, accessed December 1, 2015, <http://www.ibtimes.co.in/mallu-cyber-soldiers-retaliates-by-hacking-pakistan-governmnet-websites-648278>.

⁹⁹ Nicole Perlroth, "In a Global Market for Hacking Talent, Argentines Stand Out." *The New York Times*, November 30, 2015, accessed December 1, 2015, <http://www.nytimes.com/2015/12/01/technology/in-a-global-market-for-hacking-talent-argentines-stand-out.html>.

¹⁰⁰ Ibid.

But that is changing. In Kenya by 2017, for example, 80% of citizens will have mobile broadband subscriptions.¹⁰¹ As increasing numbers of Africans go online in 2016, the cyber attack surface will increase, and with it we will see more attacks coming from, and directed to, Africa.¹⁰²

CYBER-THREAT TRENDS

The primary trend in technology that leads to threat is constant innovation, along with the geographic and technological spread of that innovation. One example of an innovation that has increased risk is a new website, shodan.io, that serves as a search engine for the Internet of Things (IoT). Everything connected to the internet, from Minecraft stations to nuclear power plants, should theoretically be accessible from this website.

The Internet of Things

We searched shodan.io for a few minutes in November and were able to find two I.P. addresses for a Hitachi nuclear power company in the United Kingdom called Horizon Nuclear Power. A skilled hacker would be able to use those I.P. addresses, and possibly some spear-phishing techniques, to obtain access to their systems, and possibly to broader (and currently operational) Hitachi nuclear power plants. The Internet of Things, including military equipment machine-to-machine (M2M) communications,¹⁰³ and increased mobile platform usage, including mobile payment vulnerabilities, will develop quickly in 2016, and be vulnerable to search methods such as shodan.io.

Blastware, Ghostware, Ransomware, Onion Attacks, and Evoware

But shodan.io is just a single innovation. During Q3 2015, an average of 230,000 new malware samples were released onto the internet every day.¹⁰⁴ Growing forms of malware in 2016 will likely include blastware designed to destroy data and systems upon detection, ghostware designed to hide its own forensic tracks, and two-faced malware designed to act normally when being sandboxed upon startup, but change into active malware when no longer under

¹⁰¹ PKF and United States International University-Africa. *Kenya Cyber Security Report 2015: Achieving Enterprise Cyber Resilience Through Situational Awareness*. By Paula Musuva Kigen et. al. (Nairobi, Kenya: 2015), accessed November 30, 2015, <http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf>.

¹⁰² Tomi Oladipo, "Cyber-crime is Africa's 'next big threat', experts warn." *BBC News*, November 17, 2015, accessed November 30, 2015, <http://www.bbc.com/news/world-africa-34830724>.

¹⁰³ John P. Mello Jr., "M2M Offers Hackers a New Frontier for Mischief." *Network World*, February 11, 2013, accessed November 28, 2015, <http://www.networkworld.com/article/2163452/byod/m2m-offers-hackers-a-new-frontier-for-mischief.html>.

¹⁰⁴ Phil Muncaster, "Q3 sees 21 million new million new malware samples," November 20, 2015, accessed 12/2/2015, <http://www.infosecurity-magazine.com/news/q3-sees-21-million-new-malware/>.

examination.¹⁰⁵ Exploit kits that lay in wait on DNS-registered domains, and then passively infect users with malware or grayware (that imposes unwanted advertising, for example), increased in late 2015 and will likely continue to grow in 2016.

Ransomware is a relatively new form of cyber-crime in 2015 that will likely expand in 2016. This type of malware uses encryption to lock the computer, tablet, or phone's drives entirely unless a sum is paid to the criminal online.

While we have not seen much ransomware targeting the internet of things, it is highly possible to expand over the next few years. Vehicles, medical devices, and industrial control systems could all be hacked and a ransom demanded in order to return these safety-critical objects and systems to an original state of health. We might also see the rise of cyber-rent, or cyber-protection paid to cyber-criminals who agree not to hack certain items in exchange, for example, for regular and untraceable Bitcoin payments.¹⁰⁶

Onion-attacks, in which recent attacks rely upon previously hidden infections, will increase in 2016. Onion attacks are some of the most difficult to root out of a system because of their complexity and the hidden nature of their underlying backdoors.¹⁰⁷ As malware infections layer on top of one another, onion attacks will lead to increased lack of cyber-security in 2016.

The use of artificial intelligence methods, or automated genetic algorithms, to create millions of new forms of random malware, is approaching. Rather than writing each piece of malware by hand, a program could be designed to produce, replicate, and evolve new forms of "evoware" continuously such that the human programmer is no longer needed. The genetically-fit evoware produced by such a method would survive and replicate more quickly than defenses could be produced – a potential doomsday device for the internet.

The Encryption Battle

Encryption is essential for individual and organizational privacy against hackers and malicious government entities. Encrypted currencies, such as BitCoin, have been used for easier cross-border money transfers. They have given banking access to some groups that are being discriminated against, such as women in Afghanistan.

However, terrorists and criminals can hide among the anonymity of law-abiding encryption and crypto-currencies when legitimate governments have no access to encrypted communications. Encryption is increasingly being used by cyber-terrorists and cyber-criminals, making it more difficult than ever for law enforcement to track cyber-threats.¹⁰⁸ Some technology companies, like Apple and Google, are providing standard encryption on smart phones such that neither

¹⁰⁵ "IoT attacks and evasion techniques will characterize threats in 2016." *Help Net Security*, November 25, 2015, accessed November 30, 2015, <http://www.net-security.org/secworld.php?id=19152>.

¹⁰⁶ Tatsiana Yablonskaya, "Hackers attack Greek banks demanding ransom in bitcoin," December 1, 2015, accessed 12/1/2015, <http://www.coinspeaker.com/2015/12/01/hackers-threaten-greek-banks-demand-ransom-in-bitcoins/>.

¹⁰⁷ Michelle Alvarez, "Infographic: The Top Four Cybercrime Trends Are..." *Security Intelligence*, November 18, 2015, accessed November 19, 2015, <https://securityintelligence.com/infographic-the-top-four-cybercrime-trends/>.

¹⁰⁸ Sam Jones, "Rise of encryption tests intelligence Isis fight." *Financial Times*, November 18, 2015, accessed November 19, 2015, <https://next.ft.com/content/21c36512-8e15-11e5-8be4-3506bf20cc2b>.

they, nor the government, will have access to any data other than metadata on all accounts of those companies. This has allowed criminals and terrorists to hide in the crowd of new encryption users, and denied the U.S. and other legitimate governments access to large amounts of key surveillance data that has subsequently gone dark.¹⁰⁹

Crypto-currencies are increasingly used for illicit money transfers by cyber-criminals and terrorists. Despite the November 29, 2013 collapse of a BitCoin bubble after its high of \$1,137, and a host of new crypto-currency market entrants, the value of BitCoin stabilized in 2015, and even reached a one-year peak of \$448 per BitCoin on November 3, 2015. As of November 19, 2015, the hundreds of crypto-currencies tracked by coinmarketcap.com had a combined market capitalization of \$5.3 billion, \$4.8 billion of which comprised the market capitalization of bitcoin alone.¹¹⁰ The market capitalization of bitcoin shows the value people place, or expect will be placed, in an anonymous currency that moves easily across boundaries and is relatively immune to government regulation. It is, coincidentally, a perfect store of value for criminals.

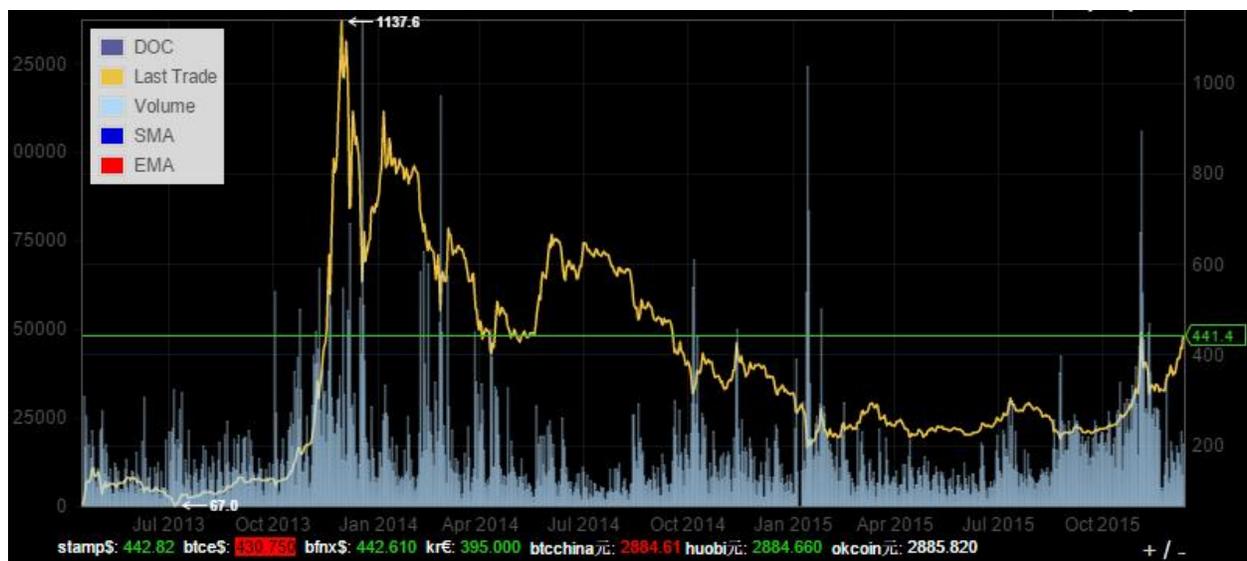


Figure 5: BitCoin price from 2013 to 2015. Source: *Bitcoin Ticker*, accessed December 11, 2015, <http://bitcointicker.co/>.

Reports claim that cyber-criminals and terrorists used Bitcoin, for example, to steal Home Depot credit cards, to fund the November Paris attacks, and as the required ransom in ransomware attacks.¹¹¹ Ghost Security Group, a collection of hacktivists, claims they located a \$3M USD

¹⁰⁹ Nicole Perloth and David E. Sanger, "F.B.I. Director Repeats Call That Ability to Read Encrypted Messages Is Crucial." *The New York Times*, November 18, 2015, accessed November 30, 2015, <http://www.nytimes.com/2015/11/19/us/politics/fbi-director-repeats-call-that-ability-to-read-encrypted-messages-is-crucial.html>.

¹¹⁰ "All Currencies." *Crypto-Currency Market Capitalizations*, accessed November 19, 2015, <http://coinmarketcap.com/all/views/all/>.

¹¹¹ Asif Intiaz, "Interpol Would Focus on the Use of Bitcoin in Cybercrime." *Payment Week*, November 18, 2015, accessed November 19, 2015, <http://paymentweek.com/2015-11-18-interpol-would-focus-on-the-use-of-bitcoin-in-cybercrime-8882/>; "New UK Cybercrime Report Makes No Mention of Bitcoin." *Blockchain Agenda*, October 17, 2015, accessed November 19, 2015, <http://insidebitcoins.com/news/new-uk-cybercrime-report-makes-no-mention-of-bitcoin/35367>.

bitcoin account linked to ISIS.¹¹² In November, Hackers called the Armada Collective threatened to take down the websites of Greek banks unless those banks each paid 20,000 bitcoin (about \$7 million USD).¹¹³

We can expect bitcoin and other cryptocurrency market capitalization to increase in 2016 as cyber-criminals and terrorists discover ways to monetize their activities, and store value in cyber-space. Major criminal syndicates may in future choose lower-cost alternates to bitcoin that they can buy cheaply, and then inflate in value by requiring that ransom or other payments be paid in that form. This is a high-risk strategy for cyber-criminals, as low initial trading volumes will more easily point blame in their direction, but it is ultimately more lucrative if executed using strong encryption and full anonymity.

HUMAN SOLUTIONS TO CYBER-RISKS

The immense attack surface upon which cyber-criminals, terrorists and irresponsible states can operate is daunting. However, humanity can and must overcome these risks through creative solutions and layered security. These solutions will include technical, legal, and policy approaches to decreasing cyber-risk.

Technical solutions to cyber-risk will include the constant evolution of security software, including through artificial intelligence, self-programming computers, and genetic algorithms. Situational awareness, detection of anomalous behavior and intrusion, layered protection from intrusion, resiliency, and operating systems must constantly evolve to stay ahead of the rapidly developing threats. Some measures will be incredibly simple and intuitive: critical infrastructure systems should be kept offline except when absolutely necessary.¹¹⁴ These measures should be applied to defense capabilities, industrial control systems, supply chains, and consumer cyber-necessities.

But ultimately, the attacker has the advantage over the defender. The attacker focuses attention and resources on single points of entry, whereas the defender must secure the entire potential attack surface.

This report is not focused on technical defensive solutions that have limited capacity by the nature of the field of cyber-security. Instead, we focus on legal and policy solutions that will enable the security technicians, and deter the bad actors.

¹¹² Heather Nauert, "ISIS parks its cash in Bitcoin, experts say." *Fox News*, November 25, 2015, accessed November 30, 2015, <http://www.foxnews.com/tech/2015/11/25/isis-parks-its-cash-in-bitcoin-experts-say.html>.

¹¹³ Tatsiana Yablonskaya, "Hackers attack Greek banks demanding ransom in bitcoin."

¹¹⁴ Megan Eckstein, "NAVEA Working Towards Cyber Detention, Protection Tool for Shipboard Systems." *USNI News*, November 13, 2015, accessed November 13, 2015, <http://news.usni.org/2015/11/13/navsea-working-towards-cyber-detection-protection-tool-for-shipboard-systems>.

Legal Solutions

Cyber-terrain lies largely outside the laws of war for terrorists,¹¹⁵ and experts disagree on the appropriate amount of regulation (whether or not it is possible) for online content and activities. But the threat is sufficient that even China and Russia, countries which have gained much through their state-sponsored cyber-crime, are at least claiming to seek more oversight.¹¹⁶ The threats are real and must be addressed on a global basis through a multi-stakeholder and multi-national approach, including the technology industry, government and international organizations.¹¹⁷

Regulation of Bitcoin and other cryptocurrencies, and the possibility of making them illegal, should be studied. Cryptocurrencies damn the public if they do, and damn the public if they don't. If cryptocurrencies work, they remove demand and therefore value from legitimate currencies -- value that would otherwise redound to the citizens of the states whose currencies decrease in value. If cryptocurrencies eventually fail, they were an expensive experiment that led to large losses to unsuspecting consumers, investors, and users. Pilot projects to regulate cryptocurrencies are a step in the right direction. New York, for example, is planning to require registration of cryptocurrency exchanges, possibly as early as 2016.¹¹⁸

Cyber-insurance is an excellent solution to many cyber-threats, and the market is responding accordingly. Increased demand for cybersecurity insurance follows predictably after each major cyber-attack on corporate targets. According to Lloyds of London, one of the world's biggest insurance companies, cyber-attacks and the resulting disruption have cost businesses \$400 billion USD annually. In 2014, insurance industry revenue from hacking insurance was a fraction of that -- \$2.5 billion USD. But insurance revenue has grown since past years. In 2013, it was \$2 billion USD, and in 2012 it was only \$1 billion USD.

As some of the biggest hacks have occurred in 2015 and 2016, we can expect cyber-insurance revenues to grow more quickly, but to continue to lag far behind total losses. Premium revenues will be unable to cover most liabilities unless consumer-level micro insurance can be developed -- requiring a very difficult verification procedure. Perhaps including cyber-insurance in small business, property, and renter's insurance will begin to close the gap in 2016. In addition to being concentrated in large companies, 90% of cyber-insurance is purchased by U.S. firms. Other companies around the world are left increasingly vulnerable.

The caps on cyber-insurance are relatively low given the massive loss of market capitalization that companies risk in cyber-space. Lloyds' maximum underwritten value is \$300 million USD,

¹¹⁵ Harold Hongju Koh, "International Law in Cyberspace," *U.S. Department of State*, September 18, 2012, <http://www.state.gov/s//releases/remarks/197924.htm> (accessed Sept. 18, 2015).

¹¹⁶ Joseph S. Nye Jr, "From bombs to bytes: Can our nuclear history inform our cyber future?" *Bulletin of the Atomic Scientists* 69. 5, (2013): 8-14.

¹¹⁷ "A global response to cyber-terrorism," *The Economist*, November 20, 2003, <http://www.economist.com/node/2187754> (accessed Sept. 18, 2015).

¹¹⁸ Shane Ferro, "Bitcoin regulation is coming to New York." *Business Insider*, April 24, 2015, accessed November 19, 2015, <http://www.businessinsider.com/bitcoin-regulated-in-new-york-2015-4>.

and the company underwrites approximately 10% of the market.¹¹⁹ Cybersecurity insurance could be backstopped by government guarantees, thus increasing maximum underwritten values and the percentage of the market underwritten. However, simple government subsidy of such a backstop should be avoided. It will incentivize lack of security and unreasonable cyber risk-taking by subsidized firms.

Examples of such government subsidy for catastrophic risk are Federal Emergency Management Agency subsidies of various forms of natural disaster insurance, and the Terrorism Risk Insurance Act (TRIA) of 2002. The government accepts 85% of the liability for qualifying terrorism insurance, but only receives 3% of the premium revenues. If the government does act as a backstop for cyber-insurance, it should avoid the TRIA mistake and, when assuming 85% of the risk, it should obtain 85% of the premiums.

Regulations should be explored that would require critical industry to have a Chief Information Security Officer (CISO), written security procedures, multi-factor authentication, data encryption, annual testing, vulnerability assessments, and strong additional protections for customer data as threats evolve.¹²⁰ A requirement to fill the Chief Information Security Officer (CISO) role, for example, is being explored in 2015 by New York City and Japan, among other authorities.¹²¹

Currently, cyber-surveillance and hacking software is relatively unregulated on the international market. Exfiltration software, designed to extract data from a target's computer, is of particular concern. Hacking Team, a Milan-based hacking and surveillance group, was exposed in 2015 for selling surveillance and hacking software to Sudan, as well as other repressive regimes. Gamma Group International, a UK company, similarly sells its FinFisher surveillance software. These tools have also been transferred to the autocratic regimes of UAE, Syria, and Bahrain. Export controls should ensure that cyber-surveillance and exfiltration software are restricted to legitimate states in good standing on human rights issues, and that cyber-security companies should have only necessary and registered access to intrusion and exfiltration software.¹²²

Policy Solutions

Significant cyber-attacks will be directed against commercial entities in 2016, including critical entities such as infrastructure and banking. Success of such attacks, which may or may not be black swan (low probability and high cost) events, could lead to damages well in excess of \$50 billion USD, or 2,500 fatalities.

¹¹⁹ Stephen Gandel, "Lloyd's CEO: Cyber attacks cost companies \$400 billion every year." *Fortune*, January 23, 2015, accessed November 28, 2015, <http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>.

¹²⁰ Liz Moyer, "New York Regulator Seeks Proposal to Improve Cybersecurity." *The New York Times*, November 10, 2015, accessed November 26, 2015, <http://www.nytimes.com/2015/11/11/business/dealbook/new-york-regulator-seeks-proposals-to-improve-cybersecurity.html>.

¹²¹ Accessed November 26, 2015, <http://www.nytimes.com/aponline/2015/11/08/world/asia/ap-as-japan-cybersecurity.html>.

¹²² Andy Greenberg, "Hacking Team Breach Shows A Global Spying Firm Run Amok." *Wired*, July 6, 2015, accessed November 30, 2015, <http://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/>; Kim Zetter, "Why an Arms Control Pact Has Security Experts Up in Arms." *Wired*, June 25, 2015, accessed November 27, 2015, <http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/>.

Critical entities should be required by law to provide information on these types of attacks, even when they are not successful or only exist in risk analyses, to government entities that can aggregate the information in order to better protect the economy and citizens. The Cybersecurity Information Sharing Act provides for such reporting and should be supported by the public and business groups whose economic margins depend on secure consumers and information infrastructure.¹²³

We have spoken much of defensive measures that can be taken to improve cyber-security. But in cyber-security we believe the best defense is a good offense and actionable intelligence. We are likely to see higher budgets for intelligence, and offense-related preparations by NATO members in 2016. The U.S. Congress released a report on November 18, 2015 stating that the U.S. should hack back against China, for example to erase stolen industrial and PII data. Such attacks should of course be legally compliant, and first ordered by a U.S. court.¹²⁴

U.S. Cyber-Command has probably the most effective cyber-offensive capabilities of any nation, most of which is closely held confidential methods. Too early utilization of these methods could cause blowback and reveal important technologies to the adversary, ruining their efficacy in an emergency.

The United Kingdom is following suit. They announced in November 2015 a plan to increase not only cyber-defense spending, but cyber-offense spending as well. The U.K. cyber-budget will double to \$2.9B USD from 2016 to 2020.¹²⁵

Public-private partnerships will increase in 2016, as governments seek to fund cyber-security start-ups for \$1M to \$3M USD. In-Q-Tel of Arlington, VA will continue to fund cyber-security private-public partnerships in 2016 in the United States. They started such funding in 1999. The U.K. funding will include a total of \$250M USD in seed capital for dozens of startups to increase innovation in the British cyber-security realm from 2016 to 2020.¹²⁶

Improved specifications, standards, and certifications must be developed for critical commercial and government entities. NATO, United States Cyber-Command and the Department of Homeland Security have to some extent in the past, and should to a greater degree in the future, play a coordinating function for participating critical commercial, academic, intelligence, military, allied, national laboratory and other government expertise to rapidly pool knowledge, develop continually improving and evolving specifications and standards, and disseminate such standards broadly back into these critical communities.

¹²³ Kery Murakami, "Banks Urge Removal of Cyber Bill Provision Allowing DHS Oversight." *Bloomberg BNA*, November 13, 2015, accessed November 13, 2015, <http://www.bna.com/banks-urge-removal-n57982063510/>.

¹²⁴ Lauren Walker, "Report: U.S. Should Fight Back When China Cyber-Attacks." *Newsweek*, November 18, 2015, accessed November 30, 2015, <http://www.newsweek.com/china-news-china-cyber-attacks-china-cyber-security-china-hacking-china-hacks-395966>.

¹²⁵ Michael Holden, "Britain to build cyber attack forces to tackle IS, hackers." *Reuters*, November 17, 2015, accessed November 30, 2015, <http://uk.reuters.com/article/2015/11/17/uk-britain-security-cybersecurity-idUKKCN0T600920151117>.

¹²⁶ Parmy Olsen, "U.K.'s Own 'DARPA' Will Pour £165 Million Into Cyber Security Startups." *Forbes*, November 17, 2015, accessed November 30, 2015, <http://www.forbes.com/sites/parmyolson/2015/11/17/uk-165-million-darpa-fund-cyber-security-startups/>.

Cyber-defense organizations of national and international bodies should hold more frequent and regular table-top, drill, and red-team exercises. For example, NATO held a cyber-security drill at a cyber-range near its cyber-security headquarters in Tallinn, Estonia in November. Thirty-three countries sent 400 representatives to simulate an attack scenario in which high-ranking officers' tablets, computers, and other devices were under cyber-attack.¹²⁷ These drills need to occur more often, and with a higher level of technical sophistication, including through computer simulations and multi-red team exercises.

Most major technology companies, and increasingly non-technology companies with a major interest in cyber-security, are offering bug bounties to hackers who find and report, privately, the existence of cyber-security vulnerabilities. United Airlines, for example, provided a million free miles to each of two hackers who provided information to the company on its cyber-vulnerabilities in July 2015. The miles will buy the hackers dozens of domestic flights.¹²⁸ This is cheaper than hiring private white-hat hackers, and likely puts white hats in a more realistic environment -- that of an actual hacker. It is not a substitute for cyber-security professionals on the payroll, and could incent malicious hacking, but bug bounties are additional layers in a layered security approach to cyber-security that should be considered.

Outreach should be made to the general public, and especially youths, on cyber-security and responsible use of the internet through events and codes of conduct. The U.S. Federal Bureau of Investigation named October as National Cyber-Security Awareness Month.¹²⁹ As we have seen that much hacking and cyber-crime originates in the anonymous underbelly of the internet, addressing negativity in these subcultures, and encouraging impressionable minds to stay away from dangerous influences, will be recognized as increasingly important in 2016.

Boston Global Forum (BGF) has joined this process by establishing our first Global Cybersecurity Day on December 12, 2015, as well as an Ethics Code of Conduct for Cyber Peace and Security, which encourages citizens to voluntarily pledge to choose clean and pure approaches to responsible use of the internet.¹³⁰ Vietnamese Prime Minister Nguyen Tan Dung is among the world leaders who praised BGF's cybersecurity initiative. He said: "The government of Vietnam acclaims the Global Cyber-Security Day initiative and highly appreciates the building of the Ethics Code of Conduct for Cyber Peace and Security initiated by policy makers, scholars and professors of the Boston Global Forum." Cyber-security Day and the Ethics Code of Conduct are envisioned, above all, to be opportunities for education and a chance to pledge support for an ethical use of the internet. According to Professor Carlos Torres, the UNESCO chair of Global Learning and Global Citizenship Education at UCLA,

¹²⁷ "Estonia hosts NATO cyberdrill with focus on infected tablets." *The Washington Post*, November 19, 2015, accessed November 30, 2015, https://www.washingtonpost.com/world/europe/estonia-hosts-nato-cyberdrill-with-focus-on-infected-tablets/2015/11/19/2638d0a2-8ecc-11e5-934c-a369c80822c2_story.html.

¹²⁸ Chris Fox, "United hackers given million free flight miles." *BBC News*, July 16, 2015, accessed November 28, 2015, <http://www.bbc.com/news/technology-33552195>.

¹²⁹ "National Cyber Security Awareness Month." *The Federal Bureau of Investigation*, October 1, 2015, accessed November 30, 2015, <https://www.fbi.gov/news/stories/2015/october/national-cyber-security-awareness-month/national-cyber-security-awareness-month>.

¹³⁰ Boston Global Forum. "Vietnam's Prime Minister Calls for a Clean and Pure Internet on the Global Cyber-Security Day," accessed 12/1/2015, <http://bostonglobalforum.org/blog/2015/11/vietnam-prime-minister-supports-the-global-cyber-security-day/>.

“Global Cybersecurity Day and the Ethics Code of Conduct for Cyber Peace and Security comprise a wonderful initiative that creates synergies with our Global Citizenship Education Program.”

International cooperation on youth outreach, law enforcement and defense should be increased. The United Nations and the G-20 group of nations have affirmed that international law, for example concepts of proportionality and discrimination, apply in cyber-space. This means that the civilian damage done by cyber-attacks, to comply with international law, must be proportional to the military advantage gained, and that cyber-attacks must discriminate between civilian and military targets. State victims of cyber-attack should take aggressor states to international court for their transgressions, producing international landmark cases. An improved enforcement mechanism should be established such that the law has effect.¹³¹

But current international law is insufficient, and should be augmented by additional laws and treaties between countries. They should mandate that cyber-defense budgets include measures to: restrict attacks on critical infrastructure and civilian assets,¹³² help any country under malicious cyber-attack, agree to let emergency response teams work unimpeded, increase transparency of cyber policies, and establish hotlines for use during cyber crises. Additional international and treaty law should establish pledges of: no first use of cyber weapons against civilian targets, norms of self-restraint, and vows to disclose zero day vulnerabilities in a timely manner.¹³³

The Wassenaar Arrangement, agreed by 41 countries including most of Western Europe and North America, was originally intended to control weapons of mass destruction. But since 2013 the agreement is being extended to cyber-surveillance and intrusion software. These types of agreements are making change in the right direction, but they need to better take into account the opinions of, and potentially unreasonable strictures they might impose upon, cyber-security professionals.¹³⁴

Policy makers can improve cybersecurity skills to decrease labor market shortages by encouraging computer science, computer engineering, and related majors in not only universities, but as courses of study in high school. Through regulation and budget prioritization, policy makers can also require companies and government agencies such as U.S. Cyber-

¹³¹ Ellen Nakashima, “World’s richest nations agree hacking for commercial benefit is off-limits.” *The Washington Post*, November 16, 2015, accessed November 30, 2015, https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

¹³² United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. (Seventieth session, July 22, 2015), accessed November 30, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

¹³³ Joseph S. Nye Jr., “The world needs new norms on cyberwarfare.” *The Washington Post*, October 1, 2015, accessed November 30, 2015, https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html.

¹³⁴ Ibid.

Command to hire more cyber security personnel, thereby increasing demand signals felt by the labor market, unemployed, and students choosing majors.¹³⁵

However, care should be taken when increasing labor market demand for cyber-security experts, such that increased demand does not thereby incentivize youth to become hackers in order to gain cyber-security skills for the legitimate cyber-security labor market. Solving this negative second-order effect of increasing cyber-security budgets will require further research.

Individual countries have incentives to turn a blind eye to their own international cyber-criminals - who, after all, increase GDP at the expense of other countries, some of which may be adversaries. Therefore sanctions against such international cyber-criminality must be at the international, not just national, level. This will in the first instance include increased international transparency, in which politicians from victimized countries complain expose the unprosecuted criminal actions of international cyber-crime emanating from other countries.

When public criticism fails, as undoubtedly it usually will, the next step should be robust economic sanctions. President Obama did in fact threaten economic sanctions against China over cyber-espionage in 2015. It succeeded in getting President Xi Jinping of China to agree to a cyber-deal with President Obama in which both sides pledged not to use cyber-espionage against the other for commercial purposes. Cyber-espionage for state purposes, however, was conspicuously absent from the deal. President Xi Jinping also signed the G20 pledge against cyber espionage, this time for both commercial and state purposes.¹³⁶ Such promises have been broken in the past, and are highly likely to be broken in the future, including in 2016.

CONCLUSION

Cyber-threats are increasing exponentially as cyber-technology development continues apace. The quicker and more expansive the development of new technologies, including among the internet of things, the greater is the attack surface made vulnerable to hackers. Maintaining security in this environment will require legal and policy changes, and much greater budgetary and scientific resources provided to agencies and commands that provide security in cyberspace.

While cyber-insurance is one useful approach to spreading cyber-risk, it should not be subsidized by government. If the government acts as a back-stop for cyber-insurance, it should receive an appropriate percentage of the premium revenues. Increasing budgets for cyber-security are necessary to incentivize new entrants into the cyber-security field. However, care

¹³⁵ Rene Millman, "Free market is failing cyber-security, blast GCHQ chief." *SC Magazine*, November 13, 2015, accessed November 13, 2015, <http://www.scmagazineuk.com/free-market-is-failing-cyber-security-blasts-gchq-chief/article/453809/>.

¹³⁶ Ellen Nakashima, "World's richest nations agree hacking for commercial benefit is off-limits." *The Washington Post*, November 16, 2015, accessed November 30, 2015, https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

should be taken such that these new budgets do not incentivize entrants to gain skills through criminal hacking.

Defensive and insurance measures to cyber-security are necessary, but the U.S. government, NATO, and other Western nations appear to be neglecting prioritization of actionable intelligence, and the maxim that the best defense is a good offense. Good intelligence in cyberspace requires government backdoors to encrypted communications, and illegalization of technologies that enable criminals, such as crypto-currencies, surveillance software, and off-the-shelf hacking tools. Government needs to take more offensive actions against adversaries. If government can find, fix, and finish cyber-criminals, cyber-terrorists, and state-sponsored hackers, it will save the immense costs borne by society and government from expensive and relatively ineffective defensive measures.

Cyber-security is negatively affected, and perversely so, by growing cyber-security budgets focused on defensive measures. As cyber-security budgets increase for defenses against hacking, so do incentives for new labor market entrants to learn white-hat security skills that are indistinguishable from black hat hacking skills. White hats and black hats are interchangeable. White hat hackers during the day could easily go home and become black hats for extra income. For every new cyber security specialist that gets a cyber security job, those who don't get such jobs could turn to hacking, especially in regions that lack effective rule of law. As the cyber-terrain advantages the attacker, cyber-security will ironically decrease as cyber-security budgets increase.

Finally, hacking and cyber-crime has at least some of its origins in the negativity found in pervasive anonymous chat rooms and websites, often frequented by the young and impressionable. The public, concerned citizens, and cyber-security professionals should make a greater effort to understand the youth in these locations, and develop strategies for steering them towards positive academic pursuits and career goals. Ultimately, hacking, terrorism, and criminality of all sorts will not be solved until societies are able to achieve peace and security through an infusion of cyber ethics and principle into the actions and beliefs of diverse international populations.

Corr Analytics of New York City contributed to the writing of this report. Corr Analytics was founded by Anders Corr in 2013 and provides analysis to media, non-profit and business clients, with a focus on strategic and international political risk. Areas of expertise include cyber-security, international conflict, and quantitative analysis. The company has methodological expertise in statistics, surveys, modeling, simulation, and causal inference.



BOSTON GLOBAL FORUM

BEACON HILL, BOSTON, MA 02108

TEL: +1 (617) 286 6589

SKYPE: BOSTONGLOBALFORUM

E-MAIL: OFFICE@BOSTONGLOBALFORUM.ORG