THE CYBER DOMAIN

FIVE WAYS TO FRAME THE SECURITY POLICY DISCUSSION

STEPHEN RECCA, M.A.
UNIVERSITY PROGRAM DIRECTOR,
HOMELAND SECURITY

BRUCE HARMON, Ph.D.
UNIVERSITY PROGRAM CHAIR,
COMPUTER SCIENCE

Colorado Technical University.

THE CYBER DOMAIN
FIVE WAYS TO FRAME THE SECURITY POLICY DISCUSSION

In August 2010, the international pedophile ring Dreamboard was shut down and 52 arrests were made after a worldwide investigation led by the U.S. Department of Homeland Security. With about 600 members, the invitation-only website is believed to have distributed 123 terabytes of child pornography. It was the biggest prosecution by the U.S. of child pornographers.

In May 2011, the Chinese Defense Ministry confirmed the existence of the Blue Army, a team of 30 elite Internet specialists officially said to be protecting the People's Liberation Army from cyber attacks. Many worry, however, that the unit has been used to hack foreign government systems.

In March 2012, between 50,000 and 10 million credit card holders were put at risk of fraudulent charges when third-party processor Global Payments was hacked.

The last decade has introduced a myriad of technological advances, forcing a sea of change upon the world with many positive implications. But for all the positives, there's a dark side to the rapidly evolving cyber world, and these three examples just touch on its scope. There's been a simultaneous emergence of cyber threats and crimes that pose a significant risk to individuals, businesses and governments.

The combination of advancing technology and criminal sophistication makes the cyber realm a critical domain where public and private sector entities must come together to develop a defensive strategy. Of course that's no small challenge. **As quickly as technology changes, so do the threats.** Yet, the development of a coherent national policy for the cyber domain is slow. It cannot keep up with the rapid growth of technology and this creates challenges in how to best manage cybersecurity issues.

The onus is on security and technology professionals, current and future, to shape the nation's policy on cybersecurity. This involves increasing our collective understanding of the cyber domain and doing more than merely identifying future challenges, but also developing creative solutions to resolve them.

THE COMBINATION OF ADVANCING TECHNOLOGY AND CRIMINAL SOPHISTICATION MAKES THE CYBER REALM A CRITICAL DOMAIN WHERE PUBLIC AND PRIVATE SECTOR ENTITIES MUST COME TOGETHER TO DEVELOP A DEFENSIVE STRATEGY.

FIVE WAYS TO GET AHEAD OF THE CYBERSECURITY CURVE

1. UNDERSTAND THE CYBER DOMAIN

From a policy perspective, it's essential to have a firm grasp on the complex and sprawling dimensions of the cyber domain. That's no easy task given the international nature of the cyber domain and the expansive reach of its tendrils, which spread to multiple facets of our lives, culture and society.

2. DEVELOP UNIFIED LANGUAGE

When it comes to developing cybersecurity policies and processes, we need to speak the same language. This means adopting common terms easily understood by laypeople and technical experts. Communicating in a language that makes sense to a large population will let us focus on creating solutions to the issues at hand, rather than interpreting meaning.

3. IDENTIFY THREATS

We need to capture the diversity of potential cyber threats, from hacking to viruses, from organized crime to not-so-organized crime, and from cyber crime to cyber warfare. We must also delineate the issues that affect individuals versus public entities. Individuals often worry about identity theft, while larger organizations are concerned with security of data and systems. There are innumerable threats that put the cyber domain at risk – large and small – and we must identify all of them.

4. UNDERSTAND CYBER CRIMINAL BEHAVIOR

A comprehensive understanding of the behavior and motivation of these cyber criminals will enable security professionals to proactively identify potential threats before they come to pass.

5. DEVELOP NATIONAL CYBERSECURITY POLICY

Cybersecurity policy must reflect our nation's best thinking, thinking that encompasses private and public concerns in the domain. Ultimately, cybersecurity policy must meet on common ground, providing an effective and secure way to manage public and private interests in this new world of technological advancement.

1.
UNDERSTAND THE CYBER DOMAIN

Government officials share worries over cybersecurity. The Intelligence Community warns of cyber threats from nation states, anarchist groups and lone wolves. Civil liberties watch groups decry infringements of privacy and individual rights by state-sponsored cyber eavesdropping. And cyberspace experts and open-source advocates worry about cyber lockdown, through Hobbesian restrictions on web access.

This angst comes with good reason. Each of these communities views the computer software, hardware and pathway infrastructure through a different lens, with legitimate concerns on the use and misuse of this thing called "cyber." The hope is that these disparate communities can find common ground for the task of more effectively managing the challenges of the sprawling digital space. To get there, we must develop a comprehensive understanding of the cyber domain landscape.

10M
IN MARCH 2012, UP TO 10 MILLION
CREDIT CARD HOLDERS WERE
PUT AT RISK DUE TO HACKING

Source: Survey from Alumni Center Progression report, Champion College Services, September 2012.

WHAT IS CYBER?

Etymologically speaking, it's a descriptor. That doesn't provide much help, but essentially "cyber" is an adjective to describe the digital aspects of words already in your vocabulary: cyberspace, cybersecurity, cyber crime, cyberbullying, cyber friend, cyberpunk and so on. "Cyber" is simply a way to frame familiar reference points to the digital world of computer networks.

Some may argue that cyber is indefinable. That's true in practice, not theory. As far back as 1992, the Oxford English Dictionary (OED) defined cyber as: "Of, relating to, or involving (the culture of) computers, virtual reality or the Internet ..."

That seems reasonable, at least until we break down each of the subsets. These are terms we all use comfortably, but without certainty. Culture of computers? Virtual reality? Even the Internet, which some tend to confuse with the World Wide Web, presents some definition challenges.

Semantics aside, the challenge is that cyber and related activities have become part of our everyday vocabulary with the explosion of computing technology in the last two decades. As technology consumers in our professional and personal lives, we have had to learn how to use the tools, and grasp the terminology to go along with them. But, arguably, our understanding of the essential concepts in this new and essential domain is lagging far behind.

BRUSH UP ON YOUR CYBER VOCABULARY

Click the titles below to visit websites that can help bolster your understanding of the cyber playing field:

CYBER CRIME DEFINITIONS

You may not be familiar with the term SPIT, but you've probably experienced it. It's an acronym for Spam Over Internet Telephony, or all those unwanted, pre-recorded, auto-dial sales calls. Pursuit Magazine compiles this and other terms relevant to the Internet and cyber crimes.

CYBERBULLYING GLOSSARY

For parents and families who want to better understand how the digital environment contributes to the rise in cyberbullying, this site contains a lot of information and a good glossary of terms

CYBERSECURITY REPORT

For those interested in cybersecurity as a subset of national security, check out this site for its downloadable report. The publication is an output of collaboration between the U.S. and Russia. This is a particularly noteworthy effort considering the U.S. has lagged slightly behind Russia when it comes to deploying tactical and operational cyber armies.

2.
DEVELOP UNIFIED LANGUAGE

Everyone is vulnerable to cyber crime and other breaches to the security of their digital systems and identity. Our world is increasingly connected through computers, smartphones, tablets and an explosion of apps. This influx of technology results in a gateway flooded with an overwhelming number of digital portals to protect.

There is no easy, one-size-fits-all fix to the issue of cybersecurity. But an educated public is more aware of the risks, which naturally makes it better equipped to counteract potential threats. That education begins by adopting a common language around cybersecurity risks, including:

MALWARE: Any piece of software maliciously placed on a computing device. Malicious software.

WORM: A stand-alone malware program that replicates itself from one computer to another, often via the Internet.

VIRUS: Malware that corrupts the programs and data to which it is attached.

TROJAN HORSE: Malware that presents itself as a harmless "gift" but in fact is intended to harm.

ROOTKIT: Malware intended to gain administrative privileges and to do further harm.

DENIAL OF SERVICE ATTACK: Attack that floods the resources of a server or website so that legitimate users are denied the resources of the site.

KEYSTROKE LOGGING: The capture of user keystrokes, often via malware, usually for the gain of passwords and other credentials.

SPYWARE: Any use of malware to gain privileged information about the user. Keystroke logging is an example.

ADWARE: Software that presents advertising such as pop-ups.

ADVANCED PERSISTENT THREAT: Actions of a group or government seeking to systematically degrade another group over time.

ZOMBIE: Compromised computer infected with malware used under remote control to spread mayhem over the Internet.

BOTNET: Network of computers with the same malware working collectively to distribute spam or launch denial of service attacks. A collection of zombies.

FIREWALL: Software or hardware system that serves to prevent malware from penetrating a network.

ANTI-VIRUS: Software that discovers, quarantines and eliminates viruses.

PHISHING: The attempt to obtain personal information such as accounts and passwords.

SPEAR PHISHING: Phishing that targets a specific individual.

CYBER ATTACK: Any attack on computing resources.

These terms are a primer to provide a baseline for understanding cybersecurity terminology. As technology and the threat of criminal activity grow, so will this list. Staying abreast of current cybersecurity language is essential to clearly communicating the process of mitigating, managing and hopefully eliminating potential risk. Make it a point to keep up with the vocabulary as it changes.

3.
IDENTIFY THREATS

The cyber domain is vast. As a result, there is considerable flexibility in word choice and continued uncertainty in our collective understanding of the domain. What is clear is that this new operating area, which is termed "cyberspace," contains significant threats to privacy, as well as personal and national security.

There are four broad areas of concern: privacy, criminal activity, anarchist efforts and national security. Let's take a deeper look at each of these threats as they relate to cybersecurity.

PRIVACY

We tend to associate the day-to-day issues of cybersecurity, such as data intrusion, access to Personal Identifiable Information (PII), credit card fraud and theft as privacy and criminal concerns. These issues hit us at a very personal level and are both important and, unfortunately, enduring aspects of the information age. But really, these intrusions are more associated with fundamental human traits than with 21st century life. As long as there have been personal valuables, crooks have tried to steal them. Technology simply offers new methods for criminals to invade personal privacy and allows smaller groups or individuals with few resources to "box above their weight class," forcing resource-intensive countermeasures. For better or worse, gone are the days of Glenn Ford's sheriff taming the Wild West with a six-shooter and a pure heart.

CRIMINAL

On the criminal side, there are new technology threats announced daily. More recently, it was an Android app-in-the-making that captured smartphone data and displayed a 3-D history. Researchers at Indiana University, working with the Naval Surface Warfare Center, developed a camera app – really, malware – that secretly records a user's actions and data by taking periodic photos. The smartphone is temporarily muted, so the owner is unaware the app is noting location and relative movement. According to a recent article, the "images could then be browsed by criminals for objects worth stealing, such as credit card details, identity-related data or calendar events that could reveal when a user might be away." This threat is worrisome, as it essentially allows access to almost every aspect of your daily life.

Concerns of fraud, theft and malicious intent are real. Most will not stop using smartphones and other devices of convenience so the Latin phrase applies: *caveat utilitor*, or "let the user beware."

CONCERNS OF FRAUD, THEFT AND MALICIOUS INTENT ARE REAL. WHEN USING APPLICATIONS AND DEVICES, THE LATIN PHRASE *CAVEAT UTILITOR* APPLIES – "LET THE USER BEWARE."

ANARCHIST EFFORTS

The traditional actions of oppositional anarchist elements are significant. But when it comes to national impact, the greatest threat comes from those wishing to challenge the power and legitimacy of the United States, and have the capacity to do so. The more obvious source of these threats is existing nation states, namely China and Russia. And, enabled by technology, lesser powers such as Iran, North Korea and anti-U.S. groups such as al-Qaeda.

NATIONAL SECURITY

The national security threat is real and current. Lieutenant General Keith Alexander, Director of the National Security Agency and head of U.S. Cyber Command, told the Senate Armed Services Committee in 2012 that Defense Department networks face an unbelievable six million attacks each day. The majority of these originate in China, with increasing numbers coming from North Korea and other parts of Asia.

Those in positions to advise governments and corporate leaders continue to sound the alarm. Eugene Kaspersky, CEO of Moscow-based Kaspersky Lab, offered a bleak portrait of a future of government-sponsored attacks and intrusions, stating that if the willingness to use malware continues,

> "SOMEWHERE IN 2020, MAYBE 2040, WE'LL GET BACK TO A ROMANTIC TIME — NO POWER, NO CARS, NO TRAINS." ACCORDING TO KASPERSKY, VIRUSES ARE BECOMING MORE ADVANCED EVERY DAY. AND, "IF PREVIOUS VIRUSES WERE LIKE BICYCLES, THEN THE STUXNET WORM THAT DAMAGED URANIUM ENRICHMENT CENTRIFUGES AT THE NATANZ PLANT IN IRAN TWO YEARS AGO WOULD BE A PLANE AND THE LATEST PROGRAMS, DUBBED FLAME AND GAUSS, WOULD BE SPACE SHUTTLES."

Stuxnet and Flame reportedly came from "the good guys." Is there any doubt that our adversaries are working hard to build the next-generation virtual cyber warriors through viruses, worms and whatever follows? The threats are serious, numerous, varied and difficult to detect and counter. Surely, we have government strategies, regulations and policies in place to deal effectively with cybersecurity. And, these government armies are collaborating side by side with the private sector, to share information and resources to keep us ahead of the game. Or, perhaps not quite yet.

4. UNDERSTAND CYBER CRIMINAL BEHAVIOR

Former U.S. Secretary of Defense Leon Panetta warned Americans of the possibility of a "cyber Pearl Harbor," a devastating attack on the computing infrastructure of the United States. It was a sobering speech to say the least. That such a high-ranking government official should make such a warning is testament to the vulnerability of our computing systems and the technology they control. He is not the first, nor will he be the last, to sound the alarm.

There is a tremendous diversity to the threats in the cyber domain. Let's take a closer look at the individuals responsible for the various cybersecurity threats.

HACKERS

Hackers are individuals who seek to demonstrate their ability to cause harm by simple exploitation of vulnerabilities in computer operating systems, networks and applications. The hackers often have no other motive than to show that they are clever enough to do it or to expose vulnerabilities to those who should know better. Hackers are behind most viruses.

DISRUPTORS

Some hackers graduate to become disruptors, or those who seek to disrupt business websites by denial of service attacks. Usually this is done without attempts to gain or to profit, but rather just a desire to cause upheaval. An individual or group conspires to bombard the relevant servers with an overwhelming number of requests so that the servers cannot serve real customers. Worms, zombies and the like are dispersed from numerous computers under either remote control or autonomous operation.

CRIMINALS

Then there are the criminals, often operating as part of a criminal organization that seeks to steal identities and to access sensitive account information, who attempt to make transactions for commercial gain. They might use phishing or social engineering to steal account names and passwords before proceeding to exploit that information.

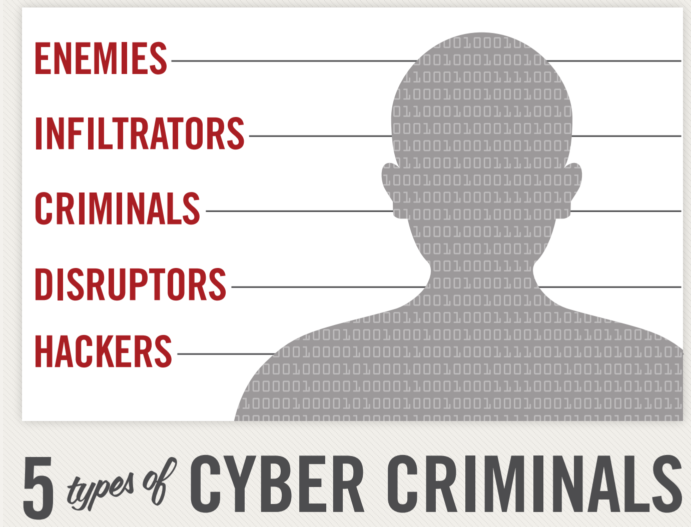
INFILTRATORS

There are also groups that seek to infiltrate organizations to find information that could then be made public for the purpose of embarrassing the penetrated organization. Sites like WikiLeaks act as ringleaders in this realm to disseminate stolen information to the public.

ENEMIES

Finally, there are nations that conspire for espionage or outright intent to damage another country. One or more nations were believed to be behind the cyber attack on the Iranian nuclear program. This attack demonstrated that even the localized programmable logic controllers that manage low-level processes could be attacked by propagation of worms over the Internet until they are resident on the actual computers that serve such controllers.

The maturation and development of cyber criminals certainly supports Former Secretary Panetta's point: it is a question of *when*, rather than *if*, an attack against the United States will occur.



5.
DEVELOP NATIONAL CYBERSECURITY POLICY

The United States does not yet have a national strategy to manage cybersecurity. Cyber law is undeveloped and while narrow segments of expertise exist inside and outside the government, broad understanding of the threat and what we might do to prepare for, respond to and recover from cyber attacks is woefully lacking. Even still, there are some things being done.

THE GOVERNMENTAL APPROACH

The federal government and the private sector, both of which have a vested interest in protecting information and sensitive operating systems, have done some good work. The current administration has provided a general overview of the government's approach to cybersecurity, which is twofold: (1) improve resilience to cyber incidents and (2) reduce the cyber threat. In addition, the White House recently released the Cyberspace Policy Review. The report provides the framework for understanding threats to the nation's communication and information infrastructure, and is a major step toward developing a national strategy.

Improving cyber resilience includes:

- Hardening digital infrastructure to be more resistant to penetration and disruption
- Improving ability to defend against sophisticated and agile cyber threats
- Recovering quickly from cyber incidents – whether caused by malicious activity, accident or natural disaster

Where possible, cyber threats must be reduced. To reduce threats, work must be done with allies to create international norms of acceptable behavior in cyberspace. This will strengthen law enforcement capabilities against cyber crime and deter potential adversaries from taking advantage of remaining vulnerabilities.

Cybersecurity strategies created for the broader public will not likely work perfectly for the private sector. Here, public entities must work in collaboration with private sector leaders to manage the threat. This will require special effort to ensure a comprehensive approach to cybersecurity, not separate strategies for the government sector and the private sector.

Nevertheless, the administration's Cyberspace Policy Review does much of what a strategy should do: provide the guiding principles for a national cybersecurity plan of action. In addition, the White House website also offers the administration's 10-point plan along with supporting documents. It's worthwhile to explore the website and also take a deeper dive into the framework documents.

The Comprehensive National Cybersecurity Initiative is also a step in the right direction. It gets to the heart of the vast challenges and puts placeholders down on how the nation might move forward to address current and future threats.

It is wise to remember, however, that cybersecurity strategies and policies cannot be government-only priorities. The private sector, as well as foreign partners, must be involved in both policy development and on-going implementation of cybersecurity measures. The administration's approach appears to be inclusive, but the devil clearly will be in the details that are yet to unfold.

DEFENSE DEPARTMENT APPROACH

The Department of Defense has long been in the game of cyber or information operations. More recently, the Defense Department has taken a keen interest in cybersecurity and defensive strategies, as well as tactics, techniques and procedures. In 2010, U.S. Cyber Command reached initial operational capability, and opened its doors for business. General Keith Alexander, head of the National Security Agency took on the dual role as commander at USCYBERCOM.

CYBERSECURITY IS AS REAL AS IT IS NEBULOUS, WHICH MEANS THERE IS A GROWING NEED FOR TRAINED, SKILLED AND FORWARD-THINKING PROFESSIONALS TO TAKE THE LEAD IN ENSURING OUR NATION'S LEADERS ARE DOING WHAT IS NECESSARY TO MANAGE THREATS.

In his statement to Congress at the time, Alexander described the playing field:

> "MY OWN VIEW IS THAT THE ONLY WAY TO COUNTERACT BOTH CRIMINAL AND ESPIONAGE ACTIVITY ONLINE IS TO BE PROACTIVE. IF THE U.S. IS TAKING A FORMAL APPROACH TO THIS, THEN THAT HAS TO BE A GOOD THING. THE CHINESE ARE VIEWED AS THE SOURCE OF A GREAT MANY ATTACKS ON WESTERN INFRASTRUCTURE AND JUST RECENTLY, THE U.S. ELECTRICAL GRID. IF THAT WERE DETERMINED TO BE AN ORGANIZED ATTACK, THE SOURCE OF THOSE ATTACKS SHOULD BE TAKEN DOWN. THE ONLY PROBLEM IS THAT THE INTERNET, BY ITS VERY NATURE, HAS NO BORDERS AND IF THE U.S. TAKES ON THE MANTLE OF THE WORLD'S POLICE; THAT MIGHT NOT BE WELL RECEIVED."

This gets to the hard truth of developing a national approach to cybersecurity: Are the cyber threats to be treated as crimes or acts of war? If it is the former, then is there a place for the Defense Department to intervene? If the latter is the case, what is our threshold for counterstrikes? What tool would we use in our military arsenal if, say, China or Iran were to attack our critical infrastructure? The best time to discuss, build consensus and develop the legal and policy frameworks, as well as the operational tools to protect and respond to these threats, is before they happen.

CYBERSECURITY STRATEGIES AND POLICIES CANNOT BE GOVERNMENT-ONLY PRIORITIES. THE PRIVATE SECTOR, AS WELL AS FOREIGN PARTNERS, MUST BE INVOLVED IN BOTH POLICY DEVELOPMENT AND ON-GOING IMPLEMENTATION.

Stephen Recca, M.A., is University Program Director for Homeland Security at Colorado Technical University. His background includes assignments with the Central Intelligence Agency, State Department and Department of Defense.

Follow his Tweets @CTUHomeland

Bruce Harmon, Ph.D., is University Program Chair for Computer Science at Colorado Technical University. He earned a Ph.D. in electrical engineering with a minor in Computer Science from the University of Colorado and his master's degree in aeronautical engineering from Purdue University. He earned a B.S. in Aeronautical Engineering at the United States Air Force Academy. After 9 years in the Air Force, he worked in defense and later at top-tier commercial companies for 17 years both in research and executive leadership positions.

Follow his Tweets @CTUTech

HOMELAND SECURITY AND CTU

Colorado Technical University is proud to be one of just a handful of universities in the United States to offer a Master's degree in Homeland Security (HLS). CTU's program is designed to provide students with a broad understanding of the homeland security enterprise at the strategic policymaking level. Geared toward homeland security practitioners, the program provides them with analytical and communication tools that can prepare them to become decision-makers in their chosen area of expertise. It has also been designed to expand students' knowledge of other disciplines within the larger homeland security enterprise, thus helping them understand the roles of given disciplines, such as law enforcement, fire, emergency services, cybersecurity and public health in the larger homeland security picture.

Colorado Technical University®

ABOUT COLORADO TECHNICAL UNIVERSITY

Founded in 1965, Colorado Technical University (CTU) provides higher education for today's career-focused students and is accredited by the Higher Learning Commission and a member of the North Central Association of Colleges and Schools. CTU's problem-based curriculum offers courses taught by real-world practitioners – many with extensive experience in the fields they teach. At CTU, students can collaborate with peers all over the country in an award-winning Virtual Campus, which was recognized as the "Best of the Best" in the Education and Academia category of the 2009 Computerworld Honors program. Students can choose from more than 100 undergraduate and graduate programs online and at campuses in multiple cities. For more information, visit www.coloradotech.edu.

Colorado Technical University cannot guarantee employment or salary. Not all programs available to residents of all states. Find disclosures on graduation rates, student financial obligations and more at www.coloradotech.edu/disclosures.