Applying Nodal Governance to Combat Cybercrime: An Novel Approach

Charles Wilson
wilsonce@udmercy.edu

Gregory Laidlaw
laidlags@udmercy.edu

University of Detroit Mercy
Center for Cyber Security and Intelligence Studies

Abstract - This paper will address the impact of the ever-increasing phenomenon of cybercrime in America. It will argue that cybercrime as a new genre of illegal behavior (criminality) is having a significantly negative impact on key aspects of America's national security, financial prosperity, and public safety. The premise of the paper is that the contemporary cyberthreat landscape is an evolving target surface with a growing cast of nation-states, transnational organized criminal organizations, and other criminal actors who are continually changing and updating their modus operandi to maintain an advantage over cybersecurity defenders. Moreover, as cybercrime incidents increase in frequency, harm, danger, and cost, the cybersecurity programs of public and private sector defenders may be incapable of effectively countering the threat, and the resulting growth in scale of cybercrime will continue to challenge and possibly overwhelm the capabilities of the federal-centric national cybersecurity strategy currently employed to counter this threat. The increasing and invasive nature of cybercrime mandates a critical and urgent need for enhanced capabilities and increased levels of expertise in combating, preventing, investigating, and policing cybercrime incidents. This paper recommends that American policymakers continue to recognize the level of threat presented by this damaging and noxious form of crime and in response adopt policies that foster implementation of an overarching national cybersecurity strategy based on the nodal governance of security. The paper recommendations that the U.S. government create operational policies and funding provisions to include and maximize the use of civil sector's capabilities and

enhance law enforcement capabilities by expanding the use of local, state, and county police agencies in the campaign against cybercrime.

Keywords

cybercrime, cybersecurity, cyberthreat, nodal governance

1 INTRODUCTION

This paper will examine the issue of cybercrime and its impact on critical aspects of American national security, economic prosperity, cybersecurity, public safety, and the lives of its citizens. The paper recommends that the U.S. government create operational policies and funding provisions to include and maximize the use of civil sector's capabilities and enhance law enforcement capabilities by expanding the use of local, state, and county police agencies in the campaign against cybercrime. This is a process called "capacity development (CD)" which is recognized in the literature as the creation of national capacity and is described as more than state-centric capacity. The CD process must recognize that the civil sector comprised of non-state actors have a legitimate role to play in the capacity development process and therefore should be part of any national CD process. It also means that our understanding of security governance needs to be one that recognizes the participation of the civil sector entities as key stakeholders, especially in cyberspace governance and cybersecurity.

The United Nations (UN) was one of the first global governance organization to recognize and conceptualize capacity development. The United Nations Secretariat defines capacity development as "the process by which people, organizations and society systematically stimulate and develop their capability over time to achieve social and economic goals, through the accession of improved of knowledge, skills, systems, and institutions – within a wider social and cultural enabling environment." The term evolved to be "community capacity building"

which defines capacity building as a long-term continual process of development that involves all stakeholders; including ministries, local authorities, non-governmental organizations, professionals, community members, academics and more. Capacity development uses a country's human, scientific, technological, organizational, and institutional and resource capabilities. The goal of capacity development is to resolve problems related to policy and methods of development, while considering the potential, limits and needs of the people of the country concerned. Capacity development takes place on an individual level, an institutional level and the societal level.

- Individual level – it requires the development of conditions that allow individual stakeholders to build and enhance knowledge, skills and abilities. It also calls for the establishment of conditions that will allow individuals to engage in the "process of learning and adapting to change.
- Institutional level – it should involve enabling existing institutions and providing the necessary support in the form of sound policies, organizational structures, and effective methods of management and revenue streams.
- Societal level – it should support the establishment of a more "interactive public administration that learns equally from its actions and from feedback it receives from the population at large." Community capacity building must be used to develop public administrators that are responsive and accountable. The computer as a target—attacking the computers of others (e.g. spreading viruses).

This paper will survey the topic through an extensive literature review and provide an in-formative summary of what the empirical literature presents as evidence of the rising menace of cybercrime. The Department of Justice categorizes computer crime, also called cybercrime, in three ways:

1. The computer as a target—attacking the computers of others (e.g. spreading viruses).
2. The computer as a weapon—using a computer to commit "traditional crime" that we see in the physical world (e.g. fraud or illegal gambling).
3. The computer as an accessory—using a computer as a "fancy filing cabinet" to store illegal or stolen information.

Moreover, the literature clearly demonstrates that cybercrime is a far more serious threat to the U.S. than many other nations, because the U.S. national security, economy, and critical infrastructure are far more dependent and operated through cyber systems than most other nations. Furthermore, there are no restrictions or limitations on the selection of a cybercrime target, as noted by Lior Kohavi (2015):

> *Cybercrime is, at its heart, a business and as with any other business, it runs on profits …. cybercrime gangs have evolved into sophisticated operation; they perform market research to understand their most lucrative market segments, use in-house or outsourced development teams to build new "product" … to drive threat penetration, and they use a complex network of distribution partners for threat delivery. (p. 1)*

2 THE SCOPE AND SCALE OF CYBERCRIME THREAT

There is no current and official source to accurately determine the true cost of cybercrime in America. McAfee (2014) estimated that the global economic impact of cybercrime was annually more than $400 billion. In America, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) tallied 269,422 complaints in 2014, totaling $800,492,073 in losses; and the center received 3,175,611 complaints since its establishment in May 2000. These estimated totals are much lower than actual cybercrime losses. The IC3 report states, "Only an estimated 15 percent of the nation's fraud victims report their crimes to law enforcement, while the IC3 estimates less than 10 percent of victims file directly through the IC3.gov. website" (p. 6). A Ponemon Institute (2014) revealed that the

average cost of cybercrime for U.S. retail stores more than doubled in 2013 to an annual average of $8.6 million per company. The annual average cost per company of successful cyberattacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries. The cost of cybercrime also should be expanded to include the more than 40 million individual U.S. citizens who suffer by having their personal identity stolen (McAfee, 2014).

The reviewed literature illustrates that America's growing dependence on technology will continue to provide a target-rich environment for the rising trend of cybercrime because information technology is used in virtually every aspect of contemporary life. According to Internet World Stats (2016) the level of Internet penetration in the U.S. is very high, with Internet users using online services to transact purchases and/or pay for merchandise via credit/debit cards linked to their banking accounts at a rate of 89.3%, ranking 1st in the world. Additionally, the U.S. is currently the largest economy in the world, which makes it the number one target for cybercriminals. The persistent increases in the frequency and severity of cyberattacks on U.S. targets show a clear threat to public and private sector entities, and individual citizens; with ominous implications for undermining U.S. institutions in the areas of national security, financial system, and public safety.

Today, the global internet population is estimated to consist of over 3.2 billion individuals (Murphy & Roser, 2017). The number of Internet-connected devices is predicted to grow fivefold by 2020, the number of connected devices growing to over 50 billion (Evans, 2012). In America, approximately 286 million individuals or 9 of every 10 American adults (89.3%) use the internet (Pew Research, 2017). By any measure, the U.S. is a prime target and fertile hunting ground for cybercriminals looking for a major score in cyberspace. Factors such as the economic level of a country, its Internet population, and the security level of the nation coalesce to define a geography of attacks (Paganini, 2012). For cybercriminals, the U.S. represents the perfect attack surface.

The perfect attack surface is comprised of a target rich environment consisting of opportunities for cybercriminals to attack victims in the public, private, and civil sectors. It should be noted and emphasized that this paper is making special note of the civil sector because that sector of American society is often overlooked and/or totally ignored in the extant literature and national policy deliberation processes related to cybersecurity. The civil sector is described and understood as:

> **Civil society** is the "aggregate of non-governmental organizations and institutions that manifest interests and will of citizens". Civil society includes the family and the private sphere, referred to as the "third sector" of society, distinct from government and business (Dictionary.com, 21st Century Lexicon).

Other literature has noted that the civil sector is the aggregation of non-governmental organizations, collective civic groups and social institutions that manifest shared interests and the will of citizens, individuals and organizations in a society. The civil sector is independent of the public (government) and private business) sectors, however, it is the catalytic agent that energizes the public and private sectors' activity in such a way as to strengthen the common good (World Economic Forum, 2013). The confluence of globalization, the Internet, and increasing rates of information exchange and technological transfer are having a significant influence on shaping global governance processes. The civil sector is playing an ever-increasing and important role in the global governance arena by creating social capital and driving policy change through what has been described as a global associational revolution. This revolution is described as a focused mobilization of organized civil sector organizations, engaging in voluntary activity across the geopolitical and socioeconomic dimensions of the world (Salamon, et al., 1999.). The revolutionary entities are comprised of an assemblage of independent and distinct civic associations, social networks, commonwealth organizations and normative groups, based on common interests, mutual trust and shared benefits that enable groups and individuals to cooperate with one another for the common good.

The rising menace of cybercrime is rapidly becoming a major concern for cybersecurity defenders who are responsible for implementing measures that will be

most effective in preventing, reducing, or mitigating the threats to computers, network systems, and any other connected devices or critical infrastructures. A retrospective examination of the number, scale and cost of cybercrime episodes illustrate that both have continued to grow at an exponential rate. For example, Security Intelligence (Kassem, 2016) stated that during 2015 cybercrime was a crime epidemic of a magnitude and sophistication that will only continue to accelerate, intensify and increase to exponential proportions in the future. The literature clearly illustrate that organized crime, transnational criminal organizations, and affiliated black-hat hackers are forming criminal networks, and have become significantly more brazen, bold and persistent in their modus operandi. Cyber criminals will continually upgrade their techniques to incorporate the very latest emerging technology into their cybercrime activities (Goodman, 2015). According to a 2014 study of the criminal groups operating in cyberspace, a full 80% of hackers are now working with or are active co-conspirators in organized criminal organizations perpetrating in cyberspace (Broadhurst, et. al., 2014). The economic damage caused by cybercrime is extremely huge and assessable. According Sameer Dixit, Senior director of Security at cybersecurity firm Spirent, in 2016 both individuals, businesses, and government agencies were struck by 90 million cyberattacks (Broadhurst, et al. 2014). The American civil sector has multiple and diverse capabilities, expertise, and skills which should be tapped by the U.S. Government as a functional enhancement to improve the overall effort in preventing, countering and responding to cybercrime attacks. According to Ghaus-Pasha (2004):

> *Civil society has been widely recognized as an essential 'third' sector. Its strength can have a positive influence on the state and the market. Civil society is therefore seen as an increasingly important agent for promoting good governance like transparency, effectiveness, openness, responsiveness and accountability (p. 3).*

3 NODAL GOVERNANCE OF SECURITY - A STRATEGIC CONCEPT FOR COMBATING CYBERCRIME

As the U.S. strives to come to terms with the increasing threat of cybercrime, the country's political leaders, policy makers, and business executives must begin to

develop and implement the right policies, laws, and strategies needed to effectively address this challenge. This paper proposes that the nodal governance of security is the appropriate strategic concept most capable of effectively answering the challenges presented by cybercrime; this paper, also, recommends that polycentric security and policing be employed as the operational and tactical framework for implementing cybercrime counter measures. Together, both concepts can be crafted and fused into an integrated approach for improving cybersecurity focused on the prevention, mitigation, and response to cybercrime. In the form of an integrated and unified strategic approach to combating cybercrime, nodal governance of security and polycentric policing offer a method for mobilizing all available resources, expertise, and capabilities.

In the development and launch of any concept of cybersecurity intended for the purpose of countering cybercrime, it is critical to harness the power and capabilities of all stakeholders, especially the private and civil sectors. Cybercriminals are equal-opportunities perpetrators, meaning they will target and attack any victim that will quickly and profitably make them money (Kohavi, 2015). In a cyber environment with ever-changing risks and threats, the government needs to do more to support the private and civil sectors, and local law enforcement in establishing robust support for cybercrime counter-measures while not creating regulations that hinder the operational freedom of those most responsible for security and policing cyberspace.

3.1 IAD-SES Framework

Professor Elinor Ostrom created an informative framework of eight design principles for the management of common-pool resources known as the Institutional Analysis and Design (IAD). The framework that she proposes can be used as a basis for collaboration and a more robust cooperative resource-sharing arrangement between the parties actively working to reduce cybercrime. By proposing a framework for sharing information and resources, it is hoped that enforcement efforts can be handled by the nodes with the needed skill, duplications of effort can be eliminated, and crimes that are not currently investigated due to

lack of expertise or geographic dispersion can be given proper attention. The rules proposed by Professor Ostrom are designed to facilitate information and resource sharing between organizations, and are as follows:

1. "clearly defined boundaries for the user pool and the resource domain"
2. "proportional equivalence between benefits and costs"
3. "collective choice arrangements [ensuring] that the resource users participate in setting… rules"
4. "monitoring…by the appropriators or by their agents"
5. "graduated sanctions" for rule violators
6. "conflict-resolution mechanisms [that] are readily available, low cost, and legitimate"
7. "minimal recognition of rights to organize"
8. "governance activities [being]…organized in multiple layers of nested enterprises." (Shackelford et Al, 2016)

3.2 Potential Governance and Policing Nodes

1. Internet users and user groups

Users can and do exert a very potent influence upon online behavior to enforce norms and report crime. Online forums and services expect and enforce acceptable behavior with the ability to limit access and ban individuals or larger groups of users. Individuals self-protect with spam, malware, and anti-virus protection, which in fact demonstrates the usefulness of nodal behavior as many of the AV and Spam protection software packages, report incidents first to the AV software vendor who then typically informs a wider audience via bulletins, blacklists, and reports to other interested groups.

2. Network Infrastructure Providers

Instructure Service Providers(ISP) act as another node through their written code of conduct or Terms of Service, which typically prohibit any criminal activity. Through the monitoring of their network, ISPs can and do detect many classes of cybercrime. Where the service provider is lax in enforcing conduct, we have seen nodal behavior from groups that provide information about an ISP and from the ISP's own customers who do not want to be blacklisted based on a ISP's lack of enforcement.

3. Corporate Entities

Non-ISP corporate entities enforce similar contractual obligations between both employees and vendors who provide services to those entities.

4. Non-governmental, non-police organizations

Many non-government organizations monitor internet activity and report to local, state, and federal agencies for potential action. These reporting agencies also disseminate information to the public. SANS ISC and SORBS are examples of non-governmental agencies that nevertheless investigate and report on cybercrime.

5. Government, non-police organizations

The Federal Trade Commission and other government agencies can fine and sanction businesses and individuals who use the internet to commit fraud or provide fraudulent information.

6. Police and Court

Whether at the local, state, or federal level, the formally recognized police are the only agencies that can apprehend and detain. The courts are the only mechanism that can determine guilt or innocence once charged.

4 SUMMARY AND CONCLUSION

While further research and refinement is required, we believe that the nodal form of governance within a polycentric framework is the basis attempting to address the difficulties of applying traditional policing methods to the cyberspace.

REFERENCES

[1] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology Vol 8 Issue 1 January - June 2014. Retrieved from http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf.

[2] Center for Strategic and International Studies. Retrieved from: https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[3] Dictionary.com (n.d.) 21st Century Lexicon. Retrieved June 7, 2017 from Dictionary.com website http://www.dictionary.com/browse/civil-society.

[4] Evans, D. (2012). Internet of Everything: It's the connections that matter. Retrieved from https://www.linkedin.com/pulse/20121201005511-122323-internet-of-everything-it-s-the-connections-that-matter.

[5] FBI's Internet Crime Complaint Center (IC3). (2014). 2014 Internet crime report. Retrieved from: https://pdf.ic3.gov/2014_IC3Report.pdf.

[6] Ghaus-Pasha, A. (2004). Role of civil society organizations in governance. Retrieved from: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan019594.pdf.

[7] Goodman, M. (2015) Future crimes: Inside the digital underground and the battle for our connected world. Anchor Books, Penguin Random House Publishing LLC, New York, NY.

[8] Internet World Stats. (2016). Internet usage statistics for all the Americas. Mini-watts Marketing Group. Retrieved from: http://www.internetworldstats.com/stats2.htm.

[9] Kassem, L. (2016). 2016 Cybercrime reloaded: Our prediction for the year ahead. Security Intelligence – Analysis and insight for information security professionals. Retrieved from: https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/.

[10] Kohavi, L. (2015). Cybercrime in North America. Retrieved from: http://www.connect-world.com/index.php/magazines/north-america/item/26462-cybercrime-in-north-america.

[11] McAfee. (2014). Net losses: Estimating the global cost of cybercrime economic impact of cybercrime II.

[12] Murphy, J., and Roser, M. (2017). 'Internet'. Published online at OurWorld In Data.org. Retrieved from: https://ourworldindata.org/internet/.

[13] Paganini, P. (2012). Cybercrime evolution in North America and Western Europe. Retrieved from: http://securityaffairs.co/wordpress/8631/cyber-crime/cybercrime-evolution-in-north-america-and-western-europe.html.

[14] Pew Research Center. (2017). Internet/Broadband Fact Sheet. Retrieved from: http://www.pewinternet.org/fact-sheet/internet-broadband/.

[15] Ponemon Institute. (2014). Cost of cybercrime study: U.S. Hewlett-Packard. Retrieved from: https://ssl.www8.hp.com/us/en/ssl/leadgen/document_download.html?objid=4AA5-5208ENW (accessed October 24, 2014).

[16] Review, (2017). Forthcoming; Kelley School of Business Research Paper No. 16-6. Retrieved from SSRN: https://ssrn.com/abstract=2715799.

[17] Salamon, L. M., Anheier, H.K., List, R., Toepler, S., Sokolowski. S.W. (1999).

[18] Global Civil Society: Dimensions of the Nonprofit Sector, Johns Hopkins Center for Civil Society Studies Retrieved from: https://www.energizeinc.com/art/global-associational-revolution.

[19] Shackelford, Scott and Raymond, Anjanette and Balakrishnan, Rakshana and Dixit, Prakhar and Gjonaj, Julianna and Kavi, Rachith, When Toasters Attack: A Polycentric Approach to Enhancing the 'Security of Things' (January 14, 2016). University of Illinois Law.

[20] World Economic Forum (2013). World Scenario Series: The Future Role of Civil Society. Retrieved from: www.forum.org/docs/WEF_FutureRoleCivilSociety_Report_2013.pdf