CYBERCRIME

A SECURITY CHALLENGE FOR THE DIGITAL AGE

PRACHISH CHAKRAVORTY | MAY 2020

Photo Credit: Cybercrime Magazine

INTRODUCTION

On a Friday morning in February 2016, a duty-manager at Bangladesh Bank, the country's central bank, noticed a problem with a printer used to produce hard-copies of the previous day's transactions for review.[1] Frustrated, but not alarmed, he decided to leave the matter as it was a long-weekend, and technical glitches like this were not uncommon.[2] Unfortunately for him, the printer malfunction was not a run-of-the-mill issue. Rather, it was part of an elaborate and sophisticated plot to steal nearly $1 billion from the central bank, through a series of unauthorized network transactions.[3] The banker, and the international community, were soon to be reminded of the profound vulnerabilities that exist in even the most secure digital systems.

In the Bangladesh Bank heist, $101 million was stolen of which $81 million was never recovered.[4] This was an enormous take, dwarfing other cyber-heists in magnitude. As a comparison, the 2018 hacking of City Union Bank in India, considered a large-scale cybercrime, netted just $1.5 million.[5] However, Bangladesh Bank could have suffered far worse. Thirty payment instructions, amounting to $850 million were flagged because the receiving bank's name was similar to an unrelated institution that was on an Iran-sanctions blacklist.[6] Furthermore, another $20 million was recovered when a transaction was held due to the recipient's name being misspelled.[7] Ultimately, luck saved Bangladesh, a poor country ranked in the bottom quarter of economies by GDP per capita[8], from a far worse outcome.

However, luck alone will not keep societies safe from the growing dangers of cybercrime. Bangladesh's central bank only moved into the digital age in the last decade.[9] International transfers that had previously occurred using teleprinters and phone lines, could now happen in a fraction of the time using an encrypted electronic payments system instead.[10] However, technological advancement often comes with new risks – and a universe of cybercriminals who seek to capitalize on our vulnerability. According to the Centre for Strategic and International Studies (CSIS), a think-tank, nearly $600 billion, or almost 1% of global GDP, is lost each year because of cybercrime.[11] As more people do more things online, on more connected devices, the risks for individuals, economies and societies becomes exponentially greater.

WHAT IS CYBERCRIME?

To understand the threat of cybercrime and how it impacts national security, it's important to first consider the nature of cybercrime itself. Although the term 'cybercrime' is used frequently in discussions among policymakers,[12] the term itself is open to interpretation and has no referent in law.[13] Instead, different organizations each define cybercrime in their own context, with disagreements over what cybercrime actually is.[14]

In essence, cybercrime describes a wide range of illicit activities, the commission of which depends on networks of information and communications technology (ICT).[15] It is a product of the digital age and closely related to the rapid expansion of digital technology. At one end of the spectrum are illicit actions that utilize digital technologies like the Internet to facilitate their commission.[16] At the other end are those that specifically require digital technology in order to occur.[17] The vast majority of cybercrimes are in-between both. Crimes like the Bangladesh Bank cyber-heist specifically required digital technologies such as the supposedly secure banking transaction network, but were also modern variants on analogue crimes of deception.

SHARED CHARACTERISTICS

Despite the wide range of activities that can be considered cybercrime, there are common characteristics among them. First, unlike many offline crimes, the risk-to-reward ratio for cybercrimes often tilts heavily in favor of the reward.[18] ICT allows cybercriminals to operate on a vast scale, identifying specifically vulnerable targets, and masking their actions in order to reap massive rewards at little risk of arrest.[19]

Second, cybercrime has no geographical limits. Looking again at the Bangladesh Bank robbery, the victim was the Bangladesh central bank, with fraudulent transaction instructions communicated virtually to banks in the United States, the Philippines and Sri Lanka.[20] Criminals can be located in one country, control computers or other devices in another, and use them to commit crimes in a third.[21]

The third commonality is the problem of attribution.[22] While sophisticated analysis can often identify the source device or devices being used to commit a cybercrime, it is much more difficult determining who was using that device and their true intent.[23] These factors make cybercrime particularly attractive to criminals and other hostile actors, and makes combatting it both more difficult and more necessary.

A GROWING MENACE

As ICT revolutionizes our lives, the risks continue to grow. The International Telecommunications Union (ITU), a United Nations agency, estimated that by the end of 2018, 51.2% of the Earth's population were connected to the internet, amounting to some 3.9 billion people.[24]

The way we connect to the internet is also rapidly expanding, as exemplified by the Internet-of-Things (IoT) phenomenon. This describes the growing number of everyday devices that are now being produced with 'smart' connectivity to the internet. The growing range of IoT devices offer new improvements in process efficiency and quality of life, but with new associated risks.[25] Between 2012 and 2018, the number of IoT devices more than tripled, and it is expected that some 50 billion devices will be connected to the internet by 2020.[26]

As our use of the internet expands and evolves, so does the nature of cybercrime. Cybercriminals have adopted new technologies quickly, capitalizing on developments like online markets and digital currencies.[27] They have also become more commercialized.[28] These developments are fueling the rise of 'Cybercrime as a Service' (CaaS), where crime is outsourced as a service, provided by those with the skills and know-how, for use by those with the funds to pay for it.[29] CaaS is facilitating a new wave of low-risk, low-cost, high-profit cybercrime on a mass scale.[30]

CYBERCRIME AND SECURITY: THE DIRECT THREAT

In the digital era, our reliance on ICT for economic, social and political activity make us both individually and collectively vulnerable to cybercrime. As a consequence, cybercrime presents a direct security challenge to governments, and requires a robust, multi-level, multi-lateral response.

The direct effect of cybercrime on security is clear and growing. Cybercrime is a mass-impact activity, with the capacity to make hundreds of millions of people victim.[31] The CSIS estimates that global losses from cybercrime increased 35% in four years, between 2014 and 2018.[32] They also estimate more than two-thirds of people online, over 2 billion people, have fallen victim to some form of compromise or theft of their personal information.[33] Research also suggests that hacking activities result in the loss of up to 780,000 records daily, and that up to 1 million new viruses and other malware products may be created each day.[34] These numbers represent the tip of the iceberg.

Mass victimization at these levels present a direct challenge to the law and order and the general stability of societies. As the criminal impacts of cybercrime expand across communities, and the ill-gotten gains from those activities in turn support other online and offline criminal activities, there is a risk of a breakdown in law and order. There will also be growing pressure from citizens for governments to address the issue; with a potential loss of state legitimacy if leaders appear unable, or unwilling, to act.[35]

THE CONVERGENCE OF BAD ACTORS: THE INDIRECT THREAT

Unfortunately, the dangers of cybercrime extend beyond the direct threat of criminality. Developments such as CaaS are lowering the barriers-of-entry, and vastly expanding the universe of actors who can engage in sophisticated cybercriminal plots. As a result, there is a new convergence of hostile actors capitalizing on the opportunities presented by cybercrime.

As the US Department of Homeland Security's Analytic Exchange Program recently reported, the proliferation of cyber-offensive capabilities and expanded array of new entrants, is reshaping the cyber-threat landscape.[36] The commodification of cybercrime is expanding the capabilities of both state and non-state actors, blurring the lines between both, and creating new opportunities for financial gain, surveillance and data collection, and cyber-warfare.[37]

In this new era, one end of the spectrum remains state actors, using their military and intelligence capabilities to conduct cyber-operations. Consider Russian and American complaints that the other is involved in an 'information war' online to undermine their regimes[38], the sophisticated 'Stuxnet' virus that sabotaged Iranian nuclear centrifuges (and was later attributed to US and Israeli intelligence agencies)[39], or persistent allegations that the Chinese government engages in industrial espionage and the theft of intellectual property, to support Chinese industries.[40]

At the other end are non-state actors that increasingly powerful and potentially more destabilizing. Transnational organized crime groups (TOCs) have the organizational ability to raise large sums of money and conduct illicit business across multiple jurisdictions.[41] By leveraging these offline capabilities online, they risk becoming a far larger threat to national governments, by effectively undermining state authority.[42]

Terrorist groups are another set of non-state actors that are expanding into cybercrime. Although TOCs and terrorist groups have traditionally avoided association,[43] cybercrime is creating new bedfellows. Terrorists increasingly engage in illicit cyber-marketplaces to source supplies and fund their activities, while TOCs seek to control and profit from those cyber-marketplaces.[44] Although their collaboration may be fleeting, terrorists in control of increasingly sophisticated CaaS tools could cause considerable harm to a state's critical infrastructure.

A third group of non-state actors are so-called 'hacktivists'. As the term suggests, these individuals and groups, are a mash-up of 'hackers' and 'activists', and engage in cybercrime in order to support or resist a political or social cause.[45] Although these vigilantes have traditionally engaged in more unsophisticated actions (such as defacing or crashing a website)[46], they are becoming increasingly more dangerous as they leverage new CaaS capabilities.

Hacktivists can also be co-opted into acting with a hostile state in an attack. For instance, in 2001 following the collision of a US spy plane and a Chinese fighter jet, Chinese hacktivists conducted a series of attacks on US government websites.[47] The Chinese government was able to deny direct responsibility while tacitly supporting the hacktivists. More recently, groups like Anonymous, have attacked the operations of financial institutions like Bank of America, MasterCard and Visa, in an escalation of their battle against restrictions on internet freedom.[48]

ADDRESSING CYBERCRIME

Cybercrime is a multi-dimensional challenge for governments. It is simultaneously a criminal matter, a national security concern, and a societal issue (for example around privacy rights) that increasingly impacts geopolitical, economic and military balances.[49.] Therefore, in order to ensure governments remain ahead of the nexus of hostile actors engaged in cybercrime, they need to cooperate and coordinate both with other foreign governments and with private businesses and civil society at home.

An urgent starting point is to elevate the importance of cybersecurity across all parts of government and to send a clear signal to all parties that developments in cybercrime are a national security priority. Governments should marshal resources commensurate to the challenge, through an all-of-government approach. In particular, this means framing cybersecurity in the broadest of terms and not just a law-enforcement or military concern. Politicians need to move away from discussing cybersecurity as 'another Cold War'[50] or akin to 'weapons of mass destruction'[51] as this unnecessarily narrows the debate to military-responses that are limited at best, and unsuitable at worst. Instead, a successful cybersecurity strategy must bring together all arms of the government to tackle cybercrime holistically.

As part of this effort, governments need to embrace three key steps to mitigate the dangers from cybercrime. First, countries need to establish new norms around cybercrime and cybersecurity. This will provide a basis for action and a collective responsibility among governments to ensure cybersecurity. A second step is to actively engage the private sector, who are often on the front-line of the fight, and third, governments need to start an open and ongoing dialogue with academia and civil society to discuss the tradeoffs involved with cybersecurity, and to set the bounds of any cybersecurity approach.

ESTABLISHING NEW NORMS

Governments must work together to define the norms of acceptable behavior regarding cybercrime. In the absence of formal rules, the default 'red-line' for many governments has been when the use of cyber-capabilities have 'consequences that lead to war.'[52] However, this extremely

broad understanding allows for a lot of behavior to be tolerated, and significant inconsistencies in how actions are perceived.[53] As more non-state actors gain the capability to commit significant cybercrimes, this red-line becomes even more meaningless.[54]

Instead, governments need to agree on clearly articulated norms around three key areas in order to set the 'ground rules' for activity in the digital age. First, they need to establish clear norms on the use of cyber-offensive capabilities by states and state-aligned agencies. Second, they need to set clear norms regarding the use of cyber-operations against private companies and citizens. Third, they need to set rules and a sanction regime around the sale of powerful cyber-capabilities. By shining a light on the CaaS trade and the impact of cybercrime on citizens and companies, the race for more dangerous cyber-tools can be slowed.

ENGAGING THE PRIVATE SECTOR

While working with foreign governments to set new norms of behavior in cyberspace, governments need to closely collaborate with the private sector to ensure citizens and companies are best prepared to deal with the impacts of cybercrime. This includes the development and adoption of best practices for companies and individuals, including regular security updates for software, investment in more defensive technologies[55] and mandated technological architecture or specific lines of code that adjust online behavior and beef-up security,[56] possibly by a newly formed cybersecurity regulator.

BALANCING COMPETING OBJECTIVES

The third pillar to combat cybercrime is to engage civil society in a meaningful dialogue around the trade-offs necessary for cybersecurity in the digital age. Unlike many other public policy discussions, cybersecurity measures can have negative and far-reaching impacts on other policy areas.[57] For instance, efforts to keep people safe from cybercrime may conflict with economic policy (by reducing connectivity and slowing the pace of online innovation), civil liberties (by reducing privacy and limiting online free speech) and national security (by enhancing state surveillance).[58] Without an honest discussion around these trade-offs, and buy-in from society as a whole, any cybersecurity strategy is at risk of public rejection.

CONCLUSION

Governments are in an unyielding arms-race with a range of state and non-state actors in the new digital era. The benefits gained from harnessing ICT in so many aspects of our political, economic and social lives, have been profound, and new technological breakthroughs continue to reshape our world for the better. But with these gains, have come new, vulnerabilities to an ever-increasing array of tools and technologies that can have direct financial effects (like the losses incurred at Bangladesh Bank), indirect societal impacts (such as increased crime online and offline) or fundamental national security implications. In order to protect citizens from these dangers, governments and their private-sector and civil-society partners need to work together across a range of platforms to better educate and prepare for future cybercrime disruptions.

Works Cited

1. Mallet, V., & Chilkoti, A. (2016, March 18). How cyber criminals targeted almost $1bn in Bangladesh Bank heist. *The Financial Times.* Retrieved from https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8
2. Ibid.
3. Ibid.
4. Ibid.
5. Hammer, J. (2018, May 3). The Billion Dollar Bank Job. *The New York Times.* Retrieved from https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
6. Ibid.
7. Ibid.
8. Central Intelligence Agency. (n.d.) Country Comparison: GDP-Per Capita (PPP). *The World Factbook.* Retrieved from https://www.cia.gov/library/publications/the-world-factbook/rankorder/2004rank.html
9. Hammer, J. (2018, May 3). The Billion Dollar Bank Job. *The New York Times.* Retrieved from https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
10. Ibid.
11. Lewis, J., (2018). Economic Impact of Cybercrime – No Slowing Down. *Centre for Strategic and International Studies and McAfee*. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime.
12. Yar, M. & Steinmetz, K. F. (2019). *Cybercrime and society.* Los Angeles; London; New Delhi; Singapore; Washington DC; Melbourne: Sage Publications.
13. Ibid.
14. Wall, D.S. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime.* doi: 10.2139/ssrn.2677113
15. Yar, M. & Steinmetz, K. F. (2019). *Cybercrime and society.* Los Angeles; London; New Delhi; Singapore; Washington DC; Melbourne: Sage Publications.
16. Wall, D.S. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime.* doi: 10.2139/ssrn.2677113
17. Ibid.
18. Lewis, J., (2018). Economic Impact of Cybercrime – No Slowing Down. *Centre for Strategic and International Studies and McAfee*. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime.
19. Ibid.
20. Hammer, J. (2018, May 3). The Billion Dollar Bank Job. *The New York Times.* Retrieved from https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
21. Singer, P.W. & Friedman, A. (2014). *Cybersecurity and Cyberwar. What Everyone Needs to Know.* New York: Oxford University Press.
22. Ibid.
23. Ibid.
24. International Telecommunications Union. (2018). *ITU Releases 2018 Global and Regional ITC Estimates*. News release. Retrieved from https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx.
25. Burhan, M., Rehman, R. et. al. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors,* 18(9), 2796. doi: 10.3390/s18092796
26. Ibid.

27. Lewis, J., (2018). Economic Impact of Cybercrime – No Slowing Down. *Centre for Strategic and International Studies and McAfee*. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime.
28. Grabosky, P. (2017). The evolution of cybercrime, 2006-2016. *Cybercrime Through an Interdisciplinary Lens.* Edited by Holt, T.J. Vol. 1. Abingdon, Oxon: Routledge.
29. Wainwright, R. & Cilluffo, F.J. (2017). *Responding to Cybercrime at Scale: Operation Avalanche – A Case Study.* Issue brief no. 2017-03. Europol and Center for Cyber & Homeland Security. George Washington University.
30. Ibid.
31. Lewis, J., (2018). Economic Impact of Cybercrime – No Slowing Down. *Centre for Strategic and International Studies and McAfee*. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime.
32. Ibid.
33. Ibid.
34. Ibid.
35. Tabansky, L. (2012). Cybercrime: A National Security Issue? *Military and Strategic Affairs.* 4(3). 117-36. Retrieved from https://www.inss.org.il/publication/cybercrime-a-national-security-issue/.
36. Department of Homeland Security. (2019). Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar. 2019 Public Private Analytic Exchange Program Report. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf
37. Ibid.
38. Singer, P.W. & Friedman, A. (2014). *Cybersecurity and Cyberwar. What Everyone Needs to Know.* New York: Oxford University Press.
39. Ibid.
40. Ibid.
41. Novakoff, R. (2016). Transnational Organized Crime: An Insidious Threat to U.S. National Security Interests. *Prism.* 5(4): 134-49. Retrieved from https://www.jstor.org/stable/26459217.
42. Ibid.
43. Ibid.
44. Ibid.
45. Singer, P.W. & Friedman, A. (2014). *Cybersecurity and Cyberwar. What Everyone Needs to Know.* New York: Oxford University Press.
46. Ibid.
47. Ibid.
48. Ibid.
49. Department of Homeland Security. (2019). Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar. 2019 Public Private Analytic Exchange Program Report. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf
50. Shachtman, N. & Singer, P.W. (2011, August 15). The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive. Article. *Brookings.edu*. Retrieved from https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/.
51. Ibid.
52. Department of Homeland Security. (2019). Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar. 2019 Public Private Analytic Exchange Program Report. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf
53. Ibid.
54. Ibid.

55. Lewis, J., (2018). Economic Impact of Cybercrime – No Slowing Down. *Centre for Strategic and International Studies and McAfee*. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime.
56. Williams, M.L. & Levi, M. (2017). *Handbook of Crime Prevention and Community Safety*. Edited by Tilley, N. & Sidebottom, A. London: Routledge.
57. National Research Council. (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, 5*, 93-98. Washington, DC: The National Academies Press. https://doi.org/10/17226/18749.
58. Ibid.