CaaS

CYBERCRIME-AS-A-SERVICE: AN EMERGING THREAT TO NATIONAL SECURITY

PRACHISH CHAKRAVORTY

APRIL 2019

Cover Image: Getty

CaaS

CYBERCRIME-AS-A-SERVICE: AN EMERGING THREAT TO NATIONAL SECURITY

Introduction

In the early 1970s, John Draper became a nationwide sensation known as ‘Captain Crunch’ after he discovered how to use a toy whistle from a cereal box to trick US telephone networks into giving him free long-distance phone calls.[1] His exploits in so called ‘phone phreaking’[2] led to several spells in prison[3] and illustrate the fact that since the earliest days of the internet and connected computers, there have been those who have sought to exploit technology for illicit gain.

Today, the threats have grown more frequent and more complex. The Center for Strategic and International Studies (CSIS), a think tank, estimates that nearly $600 billion, or almost 1% of global GDP, is lost due to cybercrime each year.[4] This vast sum is in part related to the rapid integration of cyberspace in our everyday lives. According to the International Telecommunications Union (ITU), a United Nations agency focused on information and communications technology (ITC), developed countries have seen steady growth in the percentage of population using the internet, from 51.3 percent in 2005 to 80.9 percent in 2018.[5] Globally, the ITU estimates that at the end of 2018, 51.2 percent of the Earth’s population, or some 3.9 billion people, were connected to the internet.[6]

However, our reliance on cyberspace for economic, social and political activity does not alone account for the growth in cybercrime. In addition to the increasing number of users online, the nature of cybercrime is changing, as cybercriminals adopt new technologies quickly, and capitalize on black markets and digital currencies.[7] As they do so, cybercriminals are becoming increasingly sophisticated, and commercialized.[8] These trends have coalesced into a new phenomenon of ‘Cybercrime as a Service’ (CaaS) where a service-based economy has emerged that facilitates low-risk, low-cost, and high-profit cybercrime on a mass scale.[9]

CaaS: A threat to national security

CaaS is a market-driven business model that commoditizes cybercrime tools and capabilities, and offers them to the buyers on dark web exchanges protected by the anonymity of Tor and cryptocurrencies like Bitcoin.[10] In doing so, CaaS makes highly technical cybercriminal tools and services readily accessible to those without the technical skills to develop their own, both broadening and deepening the threat of cybercrime.[11]

This paper argues that the CaaS model presents both a direct and indirect threat to the national security interests of countries like the United States. The prevalence of CaaS markets create a growth catalyst for cybercrime which in itself is a destabilizing factor for societies. Moreover, by expanding the universe of actors who can access specialized cybercrime resources, there is an increased security risk from transnational organized crime groups (TOCs), terrorist organizations, and other hostile state and non-state actors, who may use these tools against civilians, governments or national critical infrastructure. As such, CaaS is a growing danger that requires a new, collaborative responses from various levels of government and law enforcement, at the national and international level.

To understand the threat posed by CaaS, it is important to first define cybercrime and look at how CaaS has changed the way cybercriminals do business. These changes have created a risk of convergence with other malign actors, including TOCs and terrorist organizations that in turn create and amplify national security concerns. By identifying the types of threats government face, it is possible to outline some proposed solutions that work to mitigate the danger.

What is Cybercrime

The term 'cybercrime' is commonly used in public discussions and by policymakers and others.[12] However, there is no single agreed upon definition of the term and it has no referent in law.[13] Instead, there are various definitions for 'cybercrime' used by different agencies, and not everyone agrees on what it actually is.[14] There is however broad acceptance that it exists[15] – for instance, in one recent survey, 64 percent of Americans were found to have been victims of fraudulent charges or loss of personal information.[16]

Perhaps the best way to understand cybercrime is as a range of illicit activities where networks of ICT play a key role in their commission.[17] On one end of the scale, are activities that utilize the internet or cyberspace in order to assist in the crime.[18] At the other end, are those crimes that depend specifically on cyberspace and ICT in order to occur. In between are a range of hybrid activities that combine elements of both.[19]

Across this spectrum, cybercrimes share a number of common characteristics. First, they enjoy a very positive risk-to-payoff ratio, when compared to other forms of crime.[20] Smart cybercriminals can make large sums of money with very little chance of arrest or imprisionment.[21] Cybercrimes also operate on a vast scale, often using automation to identify and engage vulnerable targets. In one survey, an internet service provider reported seeing 80 billion malicious scans per day,[22] an indication of how wide a net cybercriminals often cast.

New Wine or New Bottle?

One area of debate is whether cybercrime itself is a new phenomenon, or simply old-fashion crimes conducted with new tools – what acclaimed political scientist Peter Grabosky has described as “old wine in new bottles”.[23] In this telling, the underlying crimes of fraud, theft, extortion remain the same despite the utilization of new technology and tools to commit them.[24]

This conclusion however, does not account for the changing nature of crimes committed in cyberspace. Although the types of offenses may be the same, cybercrime is transforming criminal behavior online. In some instances, as described above, there are cybercrimes that are only possible due to ICT. Crimes such as spam, click-fraud and botnets are all new in the sense that technology has created new opportunities for cybercriminals.[25]

Moreover, technology also acts as a ‘force multiplier’, making it easier through automation to conduct many multiple activities simultaneously.[26] Where traditional criminals may have committed a few large-scale crimes at great personal risk, cybercriminals increasingly use networked technology to conduct large numbers of smaller crimes, with lower risk to themselves.[27]

This difference between the nature of offline and online crimes has led to a movement away from formal, hierarchical organization structures for offline groups, such as Mafia-driven TOCs, and towards a more distributed or diffuse model of organization online.[28] It is precisely this development that has led to the CaaS phenomenon – very much new wine in a new bottle.

The impact of CaaS

CaaS markets are effective platforms for delivering cybercrime tools and services because they operate in many ways like legitimate businesses.[29] Despite being relegated to the dark web, they share similar traits to sites like eBay,[30] with features designed to promote transparency and facilitate deals. These include numerical ratings and qualitative reviews for vendors and clients,[31] the ability to make large transactions via escrow,[32] and arbitration mechanisms in the event of a dispute.[33] These innovations allow cybercriminals to focus more of their time and attention on committing crimes.[34]

As a result, CaaS has had a significant impact on the volume and diversity of cybercrime.[35] Marketplaces offer products ranging from exploit kits that automate the development and delivery of malware, to ransomware that uses encryption to remotely lock victims' data, and botnet rentals allowing cybercriminals to tap into the computing power of an army of hostage machines.[36] The result has been a staggering growth in the financial impact of cybercrime.

The CSIS estimates that global losses to cybercrime have grown from $445 billion in 2014 to $600 billion in 2018, and increase of 34.8 percent over four years.[37] By offering off-the-shelf solutions, CaaS lowers the technological barrier to entry for cybercriminals. They no longer need to rely on their own abilities and resources, but can simply buy the tools and technology required for their crimes.[38]

Expanding the Threat Universe

By making cybercrime easier to commit, CaaS has encouraged new actors to participate in cybercriminal activities, expanding the lucrative CaaS marketplace. The growth rates described above are indicative of more cybercriminals getting involved in more activities worldwide.

However, an additional threat comes from the pattern of convergence witnessed among other bad actors, including TOCs and terrorist organizations. Conventional wisdom has held that TOCs and terrorist groups generally don't associate with each other.[39] But recent examples suggest a rethink is necessary. Terrorists engage with illicit markets to fund their activities and source weapons and supplies for their operations. TOCs in turn seek out profits though illicit activities. This creates a natural convergence between the two groups.[40]

TOCs have recognized the lucrative gains to be made through cybercrime[41] and although they may only fleetingly share immediate goals with terrorist groups, their nexus is increasingly turning to the tools and capabilities available on CaaS markets to also engage in cybercrime.[42] In 2011, the US government recognized the dangers posed by TOCs and cybercrime in its 'Strategy to Combat Transnational Organized Crime'.[43] The strategy noted that through cybercrime, TOCs pose a significant threat to the integrity of financial and trust systems on which the world's economy depends.[44]

Specialization and Innovation

The commoditization of cybercrime tools and technology and development of large, lucrative CaaS marketplaces, have also had an effect on tech-savvy cybercriminals. While actors who lack the technical skills to build cybercrime tools can buy them directly, those who have the skills to develop these tools, are finding mass markets for innovative new products and services. Experienced cybercriminals are able to focus on specializing their skills, and building new, more sophisticated cybercriminal tools to meet the growing market demand for these products.[45]

As technology advances, experienced cybercriminals will develop new, more powerful and dangerous ways to conduct illicit activity online. One example is the emerging risks around 'deep fakes', the ability to use technology to create audio and video of real people doing and saying things that they never said or did.[46] Deep fakes will open up new forms of criminal exploitation and present cybercriminals with a host of new, more powerful tools and technologies that challenge the authority of the state and undermine legitimate activity on and offline.[47] This is one example of how the CaaS market model creates incentives for the rapid growth of existing cybercrime activities which in turn supports technological innovation into new, more dangerous ways to impact society.

The Challenges to National Security

CaaS marketplaces present a number of direct and indirect threats to the national security of the United States and other countries around the world. Their direct impact on society is vast and growing. Cybercrime operates as a mass-impact activity, with the capability of making hundreds of millions of people victim.[48]

One estimate from the CSIS suggests that more than two billion people, or two-thirds of people who are online, have been victim to some form of personal information theft or compromise.[49] Similarly, other estimates suggest anywhere from 300,000 to one million viruses and other malware products are created every day[50] and 780,000 records are lost to hacking daily.[51]

As governments around the world are responsible for providing law and order in their societies, these vast numbers suggest a clear and growing danger to the state's authority. As the number of victims increases, and the ways in which they are victimized becomes more prevalent, there will be growing pressure on the state to act. However, if the state is unable to curtail these impacts, and they become widespread and entrenched, there is a risk that the state will lose its legitimacy, with profound consequences.[52]

There are also indirect national security concerns raised by the CaaS model, which allows sophisticated cybercrime tools to reach hostile non-state actors like TOCs and terrorist groups. TOCs present a complex threat to the state through their ability to raise immense amounts of money and conduct illicit business across multiple borders and jurisdictions.[53] The tools of cybercrime allow TOCs to further enrich themselves, creating a danger for national security when their illicit wealth allows them to undermine governments and subvert the authority of the state.[54]

Terrorist groups, who are intent on harming the United States, also benefit from cybercrime tools and technologies, using them to raise funds and making it harder for the state to track the movement of people, goods, weapons and other materials.[55] A further danger for national security is the nature of many of the cybercriminal tools available on CaaS marketplaces. Although cybercriminals deploy technologies and services such as botnets or distributed denial of service attacks (DDoS) in order to generate income, these same tools can be retargeted towards critical infrastructure, creating new cyberterrorist threats.[56] Collectively, the growth and expansion of CaaS markets and the distribution of cybercrime tools and technologies, produce a range of risks towards national security and the safety and well-being of law-abiding citizens. Accordingly, states need to take robust, proactive measures to deal with this expanding menace.

Dealing with the Cybercrime Threat

In dealing with the rise of cybercrime, the challenge facing governments is immense. The rapid pace of technological advancement, the cross-border nature of threats and the vast amount of money involved makes any effort to deal with cybercrime fraught with difficulty. However, in conjunction with existing efforts to eradicate TOCs and terrorism, there are steps that governments can take to reduce the risk to citizens.

The proposals made here range from applying basic security measures uniformly through to challenging states that offer sanctuary to cybercriminals and their networks. Across all of these steps, states need to be actively involved in cybersecurity in order to ensure the dangers do not become more acute.[57]

As a first step, governments need to accept the dangers posed by cybercrime and send a clear signal to all parties that trends and developments in cybercrime are a national security priority.[58] This marshalling of time and resources should be directed primarily towards increased state involvement in cybersecurity coordination along with the private sector.[59] Although government cannot unilaterally secure cyberspace, it is the sole actor with responsibility for law and order, and should be an active participant in stakeholder discussions.

In some respects, implementation of basic security measures will provide a valuable line of defense against cybercrime. Governments should work towards the uniform adoption of best practices among private companies and citizens, including regularly updating security patches, open security architectures and greater investment in defensive technologies.[60]
The transnational nature of cybercrime also requires enhanced cooperation among law enforcement, both across jurisdictions and with the private sector.[61] The 'uberization' of policing is one concept that has been adopted by Europol, a leading European law enforcement agency despite having no police powers or intelligence capacity of its own.[62] Instead, it has used technology to connect to more than 500 law enforcement agencies to share information and tap resources as necessary in its fight against crime and terrorism.[63]

As the dangers of cybercrime multiply, governments should also look at adopting regulation through technology. By mandating specific forms of code, architecture or technology, regulators can subtly adjust the behavior of citizens online, in a way that is more readily adaptive to cybercriminal threats than through legislation.[64] Regulation efforts should also focus on the development of disruptive technologies that minimize the impacts of cybercrime when events do occur.[65]

A final step that states should consider, in response to the threats posed by cybercrime, is the development of a robust international legal framework and penalties for states that tacitly support cybercrime. Countries with weaker cybercrime laws suffer from higher levels of cybercrime, which in turn has an effect on other countries.[66] Governments should therefore actively support the enhancement of cybersecurity capacity in weaker countries.

However, steps should also be taken to pressure states that provide sanctuary for cybercriminals to change their behavior. Russia and North Korea for example, provide sovereign cover for cybercriminals who operate in their jurisdictions. Governments of countries like the United States and across Europe should work together to develop coordinate penalties that are painful, but reversible, in line with the dangers such state protection creates.[67]

The evolution of cybercrime as a commercial enterprise open to various bad actors, creates a compelling national security concern for governments across the globe. Although dealing with these threats will take time, investment and coordination, there must be a political and law-enforcement will to cooperate and coordinate in order to mitigate the dangers.

Footnotes

1. Markoff, John. "The Odyssey Of a Hacker: From Outlaw To Consultant." *The New York Times*, January 29, 2001. Accessed April 01, 2019. https://www.nytimes.com/2001/01/29/business/the-odyssey-of-a-hacker-from-outlaw-to-consultant.html.
2. James, Randy. "A Brief History of Cybercrime." *Time*, June 1, 2009. Accessed April 1, 2019. http://content.time.com/time/nation/article/0,8599,1902073,00.html.
3. Markoff, John. "The Odyssey Of a Hacker: From Outlaw To Consultant." *The New York Times*, January 29, 2001. Accessed April 01, 2019. https://www.nytimes.com/2001/01/29/business/the-odyssey-of-a-hacker-from-outlaw-to-consultant.html.
4. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
5. International Telecommunications Union. "ITU Releases 2018 Global and Regional ICT Estimates." News release, December 7, 2018. Accessed April 1, 2019. https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx.
6. Ibid.
7. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
8. Grabosky, Peter. The evolution of cybercrime, 2006-2016. *Cybercrime Through an Interdisciplinary Lens.* Edited by Thomas J. Holt. Vol. 1. Abingdon, Oxon: Routledge, 2017.
9. Wainwright, Robert, and Frank J. Cilluffo. *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.
10. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
11. Ibid.
12. Yar, Majid, and Kevin F. Steinmetz. *Cybercrime and Society.* 3rd ed. London: Sage Publications, 2019.
13. Ibid.
14. Wall, David S. "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime." *The European Review of Organised Crime* 2, no. 2 (2015): 71-90. Accessed April 1, 2019. doi:10.2139/ssrn.2677113.
15. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
16. Yar, Majid, and Kevin F. Steinmetz. *Cybercrime and Society.* 3rd ed. London: Sage Publications, 2019.
17. Ibid.
18. Wall, David S. "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime." *The European Review of Organised Crime* 2, no. 2 (2015): 71-90. Accessed April 1, 2019. doi:10.2139/ssrn.2677113.
19. Ibid.
20. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
21. Ibid.
22. Ibid.
23. Grabosky, Peter. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2 (June 2001): 243-49. Accessed April 1, 2019. https://journals.sagepub.com/toc/slsa/10/2.
24. "How Does the Business of Cybercrime Work?" Council on Foreign Relations. December 10, 2018. Accessed April 1, 2019. https://www.cfr.org/blog/how-does-business-cybercrime-work.
25. Tabansky, Lior. "Cybercrime: A National Security Issue?" *Military and Strategic Affairs* 4, no. 3 (December 2012): 117-36. Accessed April 1, 2019. https://www.inss.org.il/publication/cybercrime-a-national-security-issue/.
26. Wall, David S. "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime." *The European Review of Organised Crime* 2, no. 2 (2015): 71-90. Accessed April 1, 2019. doi:10.2139/ssrn.2677113.
27. Wall, David S. "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime." *The European Review of Organised Crime* 2, no. 2 (2015): 71-90. Accessed April 1, 2019. doi:10.2139/ssrn.2677113.
28. Ibid.
29. "How Does the Business of Cybercrime Work?" Council on Foreign Relations. December 10, 2018. Accessed April 1, 2019. https://www.cfr.org/blog/how-does-business-cybercrime-work.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid.
34. Ibid.
35. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
36. Ibid.
37. Ibid.
38. Robinson, Rick M. "Cybercrime-as-a-Service Poses a Growing Challenge." Security Intelligence. September 04, 2016. Accessed April 01, 2019. https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/.

39. Novakoff, Renee. "Transnational Organized Crime: An Insidious Threat to U.S. National Security Interests." *Prism* 5, no. 4 (2016): 134-49. Accessed April 1, 2019. https://www.jstor.org/stable/26459217.
40. Ibid.
41. Tabansky, Lior. "Cybercrime: A National Security Issue?" *Military and Strategic Affairs* 4, no. 3 (December 2012): 117-36. Accessed April 1, 2019. https://www.inss.org.il/publication/cybercrime-a-national-security-issue/.
42. Novakoff, Renee. "Transnational Organized Crime: An Insidious Threat to U.S. National Security Interests." *Prism* 5, no. 4 (2016): 134-49. Accessed April 1, 2019. https://www.jstor.org/stable/26459217.
43. United States. Executive Office of the President. *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security.* Washington, D.C.: Executive Office of the President, 2011. Accessed April 1, 2019. https://obamawhitehouse.archives.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf
44. Ibid.
45. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
46. Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *SSRN Electronic Journal*, July 14, 2018. Accessed April 1, 2019. doi:10.2139/ssrn.3213954.
47. Ibid.
48. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
49. Ibid.
50. Ibid.
51. Ibid.
52. Tabansky, Lior. "Cybercrime: A National Security Issue?" *Military and Strategic Affairs* 4, no. 3 (December 2012): 117-36. Accessed April 1, 2019. https://www.inss.org.il/publication/cybercrime-a-national-security-issue/.
53. Novakoff, Renee. "Transnational Organized Crime: An Insidious Threat to U.S. National Security Interests." *Prism* 5, no. 4 (2016): 134-49. Accessed April 1, 2019. https://www.jstor.org/stable/26459217.
54. Ibid.
55. Ibid.
56. Rogers, Marcus. *Routledge Handbook of Terrorism and Counterterrorism.* Edited by Andrew Silke. Abingdon, Oxon: Routledge, 2018.
57. Tabansky, Lior. "Cybercrime: A National Security Issue?" *Military and Strategic Affairs* 4, no. 3 (December 2012): 117-36. Accessed April 1, 2019. https://www.inss.org.il/publication/cybercrime-a-national-security-issue/.
58. Novakoff, Renee. "Transnational Organized Crime: An Insidious Threat to U.S. National Security Interests." *Prism* 5, no. 4 (2016): 134-49. Accessed April 1, 2019. https://www.jstor.org/stable/26459217.
59. Tabansky, Lior. "Cybercrime: A National Security Issue?" *Military and Strategic Affairs* 4, no. 3 (December 2012): 117-36. Accessed April 1, 2019. https://www.inss.org.il/publication/cybercrime-a-national-security-issue/.
60. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
61. Ibid.
62. Wainwright, Robert. "The 'Uberisation' of International Police Work." January 23, 2016. Accessed April 1, 2019. https://www.linkedin.com/pulse/uberisation-international-police-work-rob-wainwright/.
63. Ibid.
64. Williams, Matthew L., and Michael Levi. *Handbook of Crime Prevention and Community Safety.* Edited by Nick Tilley and Aiden Sidebottom. London: Routledge, 2017.
65. Wall, David S. "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime." *The European Review of Organised Crime* 2, no. 2 (2015): 71-90. Accessed April 1, 2019. doi:10.2139/ssrn.2677113.
66. Lewis, James A. *Economic Impact of Cybercrime - No Slowing Down.* Report. Center for Strategic & International Studies and McAfee. February 21, 2018. Accessed April 1, 2019. https://www.csis.org/analysis/economic-impact-cybercrime.
67. Ibid.