Centre of Excellence for National Security

Event Report

Workshop on Cybercrime

13-14 November 2017

Report on the Workshop organised by:
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University, Singapore
Supported by:
National Security Coordination Secretariat (NSCS)
Prime Minister's Office, Singapore
Rapporteurs:
Muhammad Faizal bin Abdul Rahman, Juhi Ahuja, Nur Diyanah binte Anwar, Joseph Franco, Cameron Sumpter, Dymples Leong Suying, Pravin Prakash, Romain Brian Quivooij, Tan E Guang Eugene, and Jennifer Yang Hui
Editor:
Benjamin Ang

The Workshop adheres to a variation of the Chatham House Rule. Accordingly, beyond the speakers and the presenters cited, no other attributions have been included in this report.

TABLE OF CONTENTS

Executive Summary

The Centre of Excellence for National Security (CENS) organised a workshop on 13 and 14 November 2017 titled “Cybercrime: the Hidden World”. The workshop explored new and existing methods in fighting cybercrime online and in the physical realm, assessed the psychology behind cybercrime, and studied how states around the world were coping with cybercrime.

The 13 speakers included academics, practitioners, and private sector experts from the United States, Russia, United Kingdom, France, China, India, Malaysia, and Singapore. They spoke from the perspectives of psychology, cybercrime in financial institutions, international organisations, technology, and national security.

More than 60 participants from government agencies attended the two-day workshop and participated actively in the syndicate discussions with the speakers.

The key findings from the workshop were as follows:

1. ***Cybercriminals are succeeding because of cooperation***

Economic gains are high and barriers to entry are low, making cybercrime attractive to potential criminals. They do not need be technically sophisticated because there is an ecosystem of software developers creating and selling cybercrime tools.

The greatest threat with regards to cybercrime comes from organised groups and networks that bring together individuals with specific skills to work on different fronts for a bigger criminal cause. There thus needs to be greater collaboration between law and order groups investigating the various branches of these groups to be able to better combat them.

2. Combating cybercrime is not easy, but it is not impossible

The Dark Web is often seen as a place where investigators fear to tread, and a place where laws that exist in the physical realm are easily circumvented. However, the speakers gave examples where cases were successfully prosecuted through old-fashioned police techniques such as infiltrating criminal communities.

Cybercriminals have also been captured because of human weaknesses such as pride e.g. bragging about their exploits on online forums.

3. Combating cybercrime requires cooperation across jurisdictions

The problems that exist in combating cybercrime are less technical and more political. Cybercrime is often transboundary, and requires cooperation from law enforcement agencies of multiple countries. Cybercriminals may live in (or use servers in) jurisdictions where the laws against cybercrime are weak or are weakly enforced. These criminals are able to escape capture because of the lack of cooperation and coordination between the different law enforcement agencies.

Cooperation is difficult because of procedural problems (not knowing who to contact) and differences of laws (e.g. drugs are viewed with different levels of severity). Mutual legal assistance agreements or formalised treaties against cybercrime will help. International conventions and legislation on cybercrime can reduce international attack rates. Countries

that fully embrace these conventions, allowing for greater collaboration and the sharing of information have shown the greatest reductions in attack rates.

International bodies like INTERPOL and EUROPOL are important resources that are well placed to coordinate law enforcement activities over different jurisdictions.

4. ***Combating cybercrime requires cooperation between private sector and police***

The police seek to preserve the crime scene for further investigation, which makes it difficult for the victim organization to carry on business. Private businesses seek to remediate the systems which were attacked, which makes police investigation difficult. This needs to be resolved with better cooperation.

Greater cooperation has benefits because the private sector has the skills and resources, including tools, funding and digital forensics, which police may lack, whereas police may have mutual legal assistance agreements with other countries.

5. ***Combating cybercrime requires whole of society cooperation***

There is an increasing need for greater collaboration between policy makers, law enforcement, businesses and academics. Legislation is needed for international collaboration, the criminalisation of possession, distribution and production of computer misuse tools, as well as the creation of legal obligations on the part of private firms to report cybercrimes.

Law enforcement agencies need training in cybercrime investigation, including use of tools. The public needs more awareness of cybercrime, especially the psychological factors which facilitate online abuse, cyber bullying, and ransomware attacks. When individuals and organizations have greater cyber resilience, they will be less vulnerable to ransomware attacks.

Just as cybercriminals have found success through cooperation, the key to defeating them also likes in greater cooperation between private sector, public sector, law enforcement, academics, and the general public.

Panel One: Overview of Global Cybercrime

Global Cooperation in Fighting Cybercrime
Zachary Delecki, Assistant Legal Attache, Federal Bureau of Investigation, US Embassy Singapore

Combating the proliferation of cybercrime will require cooperation from agencies within and across states, and between the public sector and private sector.

- Cybercrime proliferates where there is the greatest economic opportunity. Coupled with the fact that the economic barriers to entry are low, cybercrime offers a very attractive proposition to potential cybercriminals.

- The greatest threat with regards to cybercrime comes from organised groups and networks that bring together individuals with specific skills to work on different fronts for a bigger criminal cause. There thus needs to be greater collaboration between law and order groups investigating the various branches of these groups to be able to better combat them.

- Rather than targeting individuals that garner the most attention in these networks, e.g. hackers and coders, cybercrime agencies must work together in order to identify and target the entire organisation.

- Ransomware and 'business email compromise' scams have wreaked havoc on big firms, causing losses totalling billions and in certain instances slowing the production and delivery of critical goods and services like vaccines. These scams traditionally have been confined to big firms in the US, but in recent times, they have expanded globally and scams have increasingly targeted smaller business entities and even individuals.

- There is a need to change the paradigm of how we see these investigations. The urgency that defines counter-terrorism investigations must be combined with the methodical, legal approach of traditional, organised crime investigations to effectively battle and raise the cost of cybercrime operations.

- Creating greater trust among all stakeholders is critical to the success of cybercrime investigations, including investigative agencies within and across countries, as well as with private enterprises who are attacked by cyber criminals. This would involve coming up with a common set of definitions, norms and legal frameworks that enable agencies to work together with a common understanding.

- Public – private partnerships are critical in the fight against cybercrime, because the government doesn't often own the infrastructure that is being targeted, with critical data often in the hands of private enterprises.

Mutual Legal Assistance to Combat Transnational Cybercrime
Adam Palmer, Vice-President, Financial Services Roundtable

International cooperation on combating crime exists on several issues but continues to be dogged by procedural issues.

- While cybercriminals continue to evolve and get more sophisticated, a wide majority of cybercrime can be prevented by cyber vigilance and basic security practices. The perception that cyber criminals are “super-villains” and “masters of disguise” also needs to refuted as most cybercriminals only escape detection due to a lack of basic law enforcement capability and will to catch them.

- There exists fairly significant global agreement and cooperation on issues such as hacktivism, general cybercrime and data theft. Such consensus is harder to forge over issues such international espionage and hacking between states. It is thus important not to generalise cyber-crimes and criminal activities as being similar.

- Effective international cooperation depends on flexible procedural powers and effective lines of communication and a willingness to work together which will enable agencies to work together across borders.

- On a technical level, cybercrime cooperation is hampered by procedural, evidentiary and territorial challenges. On a procedural level, many mutual assistance requests fail because of a lack of understanding of the legal system of the state to whom the request for assistance is being made – e.g. requests are made to the wrong agency. On an evidentiary level, clarity over how evidence is obtained and an understanding of human rights norms in both states is key, otherwise the evidence obtained may not be valid in court.

- Territorial jurisdiction over which action can be taken also differs from state to state and affects the ability of states to cooperate with one another.

- Creating of cooperation frameworks is difficult and takes time and patience even amongst fairly like-minded countries. The Budapest Convention for example took a decade to negotiate and pass.

- Success in creating effective mutual assistance frameworks is dependent on getting the right people across different fields. Effective investigators alone for example would be ineffective without a well-trained legal and enforcement ecosystem

Driving Cyber Security Policy Insights from Information on the Internet
Qiu-Hong Wang, Assistant Professor, School of Information Systems, Singapore Management University

Cyber security has quickly risen to the forefront of concern for both nations and private firms and collaboration between them, despite their often-competing interests, will be of increasing importance.

- Due to the high frequency of cyber-attacks today, there has been an increasing call for greater collaboration between policy makers, businesses and experts. There is thus a need for a macro-level design on policies that will shape the internet.

- One area of interest is the question of efficacy of deterrence policies and whether domestic policies alone can be effective. International legislation too needs to be examined for efficiency. It is also necessary to decide which actors and actions should be targeted with the greatest focus to ensure the most efficient results in deterring cybercrime.

- Key areas of interest include legislation for international collaboration, the criminalisation of possession, distribution and production of computer misuse tools, as well as the creation of legal obligations on the part of private firms to report cybercrimes.

- Since the turn of the century, many countries have introduced legislation to enhance cybercrime enforcement. From 2002 to 2015, 56 countries have signed cybercrime conventions, with 52 having entered these conventions into force.

- Research has shown that international conventions and legislation on cybercrime can reduce international attack rates. Countries that fully embrace these conventions, allowing for greater collaboration and the sharing of information have shown the greatest reductions in attack rates.

- Criminalisation of production, possession and distribution of computer misuse tools helps to deter information sharing on hacker techniques and tools on hacker forums, resulting in a reduction in cyber-attacks. However, this might also have the side-effect of driving hacker collaboration further underground, making them harder to track and investigate.

- Expecting different states and commercial firms to cooperate, many of whom are competitors on different levels, is a huge challenge that will require developing effective mechanisms that do not advantage any one group over the other.

Syndicate Discussions

- **Issue: Capability of security agencies to thwart attacks and the emergence of new threats** – State agencies are now quite effective in blocking and defeating most cyberattacks on financial services. Attention has moved away from technical measures to focusing on insider threats (e.g. negligent or malicious employees). For example, while investigating a large cyberattack targeting credit cards recently, a top global bank found that one of its customer service employees was involved.

- **Issue: Personal data protection versus law enforcement requirement investigations requirements** – The issue came to the fore when the FBI sought Apple's assistance to unlock the iPhone of a San Bernardino assailant in 2014. The debate publicly highlighted the conflict between the private sector and law enforcement. However, there is more constructive collaboration between them, such as the National Cyber-Forensics & Training

Alliance (NCFTA), which has provided a platform for frequent face-to-face interactions between security agencies, from the US and abroad, and representatives of the big banks. Some of the most successful cyber cases that the FBI has handled have come out of the NCFTA.

- **Issue: The increasing use of cryptocurrencies in cybercrime** – Organised criminal groups have begun using cryptocurrencies for traditional money laundering; for example from Bitcoin to Monero and back again to further anonymise illicit earnings. All of the Dark Web markets such as the Silk Road and AlphaBay use cryptocurrencies for buying and selling of contraband. Tracking the origins and movements of these transactions is a huge challenge for law enforcement agencies. One approach is to look back at exchanges and website developments over time and try to link individuals from earlier incarnations of onion sites and above surface sites to current dark websites and operations.

- **Issue: A greater understanding of the cyber threats facing South East Asia is needed** – The capacities and approaches of countries in tackling cybercrime are very varied. Some developing countries are increasing their use of broadband connectivity without increasing their expertise in dealing with cybercrime. The legal maturity of countries could also pose challenges in enforcement and attribution efforts.

- **Issue: Aligning priorities and legislative agendas** – It is crucial to identify common goals and to work towards them. For instance, the Budapest Convention aligns legal frameworks and promotes capacity building and training. Initiatives such as a coordinated centre by like-minded countries can contribute towards establishing consolidated approaches across law enforcement such as conducting bilateral or multinational joint cyber investigations and sharing best practices.

- **Issue: More concerted approaches in harmonising global efforts** –Establishing an international root policy framework applicable on a global level could align existing efforts to tackle cybercrime. A similar equivalent to the Internet Corporation for Assigned Names and Numbers (ICANN) could be created to spearhead and coordinate such efforts. This, however, raises the possibility of countries using such capabilities for political purposes rather than cybercrime.

  Issue: Use of analysis techniques to understand online hacker forums – Machine learning with basic keywords extraction and, content analysis of phone numbers and online discussion is used to evaluate if a DDoS attack is being planned on online hacker forums. Forums are selected based on ranking by Alexa and local news reports of top-ranking forums. The key challenge is in discerning between malicious discussions and protection-related discussion as the keywords are similar. Russian online forums are more accessible, whereas Chinese forums lack in-depth discussion due to digital censorship policies. Hacker forums in the Dark Web are inaccessible, so content shared on those forums cannot be analysed.

- **Issue: Helping developing countries** – Capacity building, especially in countries where basic understanding of cyber-related issues is minimal, training and public education is key. Training must include basic knowledge on evidence collection using open source

tools, analysing the digital evidence obtained and presentation of the digital evidence for further legal action. In addition, there must be a standardised method of evidence collection and sharing among different agencies within the country and amongst different countries cross-border.

- **Issue: Identifying perpetrators and the criminal network** – For consistency across various investigation departments and various countries, the tools used for identifying perpetrators through analysing discussion data, must be kept consistent. Investigation officers and judges should be trained on using the evidence obtained for identifying the criminal network and the rightful legal action. Law enforcement agencies should expend more resources into in-depth psychological analysis techniques to identify the pitfalls leading to victimisation, which could also help to map the perpetrator's network.

Distillation

- Collaborative efforts within the South East Asia region can provide a more concerted and targeted approach to tackle cybercrime.
- New technological trends such as cryptocurrencies like Bitcoin provide both opportunities for cybercriminals especially in the dark web.
- Standardised investigative analysis and protocols should be maintained to ensure consistent investigative procedures across multiple countries and regions.

Panel 2: Cybercrime and the Dark Web

Open Source Toolkit for Cybercrime Investigators: Bitscout
Vitaly Kamluk, Director, Global Research & Analysis Team, APAC, Kaspersky Lab

The inconvenience of commercially available cybercrime investigation tools outweighs their advantages. Open-source projects carry a greater potential for sound and cheap remote digital forensics.

- Cybercrime investigations are hampered by lack of available experts and a low level of technical skills and expertise among investigators. Expensive equipment and software is also required, which can be a significant problem in some countries. As a result, cybercrime investigations grow slowly while cybercrime increases rapidly.

- Remote digital forensics (RDF) provides a wide set of technical capabilities for investigation. Additionally, RDF reduces travel time and offers instant investigation support. However, existing commercial RDF tools are prohibitive because of price and their tendency to alter the evidence. As such tools are based on automated processes, specialists who use them tend to lose their ability to manage the steps of cyber-investigations manually.

- Because of these limitations, Vitaly Kamluk and his team developed Bitscout, a customized programme that can be transported on a single CD. They designed it as a comprehensive solution that meets their requirements of reliability and usability. It is minimal in size and memory use, with a simple interface that can be used by non-skilled local staff.

- Pros and cons associated with Bitscout and commercial programmes shows that cybercrime investigation tools should be as transparent, affordable and extendable as possible. Rather than spending huge amounts in expensive proprietary tools and services, individual users and organisations that need to invest in RDF should support open-source projects.

Predators Lurking in the Cybercrime Underground
Vicky Ray, Director, Palo Alto Networks

Developers and sellers of malicious software create resources and tactics which they sell to cybercriminals. Even though they do not commit the crimes themselves, they are important enablers and accomplices.

- Cybercrime online forums are ecosystems that provide some cybercriminals with the opportunity to collaborate, develop malicious software and sell these programmes. Such forums rely on a clear division of responsibilities A typical underground forum includes malware developers, marketing services providers and attack operators, among other functions.

- “Orcus” is a sophisticated Remote Access Trojan or RAT (a malware that allows hackers to take control of one or several computers through a back door) that was

developed in 2015 under the name of “Schnorchel” and commercialised in 2016. A crucial element of cyber-investigations related to such cases is to identify the developers and sellers of malwares through the multiple names and aliases they use online.

- Building a case against cybercriminals requires a thorough knowledge of the characteristics of malware involved, such as how these programmes affect microphones recording, screen captures and webcams. Legal challenges are also involved. For instance, Orcus developers were careful not to use the programme themselves.

- The Orcus cases shows that developers and sellers of RATs and similar software play a key support role by providing cybercriminals with tools to spy and steal information, while making big profits. The sharing of investigation results and collaboration between the private sector and law enforcement agencies are keys that may lead to successful prosecution.

Is There a Light at the End of the Tunnel of the Deep/Dark Web

Christopher Church, Senior Mobile Forensic Specialist, INTERPOL Global Complex For Innovation

The Deep Web and Dark Web provide cybercriminals with opportunities for resources and action. Law enforcement agencies need to address different challenges to catch up. .

- As basic techniques for committing cybercrime can be easily accessed via YouTube tutorial videos, many individuals who wish to develop hacking skills do not even need to be connected to the Deep Web (96% of the Web that cannot be accessed via a traditional search engine) or the Dark Web (a small portion of the Deep Web that can only be explored through the use of anonymous networks such as Tor).

- The Deep Web and Dark Web are vast and complex virtual environments. They include websites providing services such as resources for peer-to-peer file sharing. These are taken down on a regular basis by the authorities, but they reappear via new proxies and under different names.

- Cyber-investigations are hampered by the long periods of time required by experts to gather evidence and follow court procedures (up to eight months or even five years in some cases). Some countries do not have the proper technical and human resources to deal with cybercrime. Specialists trained by law enforcement agencies are also likely to leave for the private sector, where salary conditions are more attractive.

- New targets are gradually emerging, such as mobile phones. As a response, emphasis should be placed on collaboration between law enforcement, industry and academia, to stay up to date with developments. The adoption of proper legislation by governments is an equally important area for action.

.

Syndicate Discussions

- **Issue: Similar to front companies set up by real-world organised crime syndicates, cybercriminals are hiding behind legitimate web services** - Operators of illicit websites often hire lawyers to write terms of service agreements and seek out loopholes to conceal and protect illegal activities. Communications are careful to appear to be simply conducting legitimate business, but when internet security researchers uncover the code, unlawful actions are exposed. However, it still remains difficult to compile a successful prosecution as alternate versions of the services offered may exist. Public-private relationships – both formal and informal – are crucial.

- **Issue: Criminal strategies may be evolving faster than the ability of authorities to keep up** – Cybercriminals know what tools security agencies use and have even established ways of attacking these forensic tool kits by creating traps to execute code which might delete evidence or wipe hard drives. Live operating systems such as Tails provide almost total anonymity, leaving almost zero footprints on the hard drive, which create problems for investigators. The only way to counter developments is for law enforcement to learn as quickly as the criminals and do their best to remain competitive.

- **Issue: Use of the Dark Web for money laundering and exchange of cryptocurrencies** – The Dark Web is slow, so some criminals may only use it for a short while before reverting to the usual open Internet. For transactions of cryptocurrencies, perpetrators prefer to use third party transaction providers who provide unique addresses for each transaction, making it challenging for security agencies to track them.

- **Issue: The actual size and depravity of the Dark Web** – Common estimates that only 6% of the internet is above surface are probably exaggerated. However, the content in the Dark Web is extremely dark. Beyond the sale of drugs and weapons, there are grisly services, for example, that offer to conduct bio-chemical experiments on human beings, even children or pregnant women, and provide results for a sum of money.

- **Issue: The obstacles of collaboration between private industry and law enforcement** – When a company approaches a police agency and asks to work together to solve a particular problem, the agency must conduct a due diligence check and involve lawyers for the signing of an agreement, which can take six months. By this time criminals have moved on to the next activity, so law enforcement needs to become more agile. In the UK, 90% of cases now involve digital forensics and law enforcement is struggling to keep pace. The free sharing of information and expertise is also a continuing problem as it goes against traditional law enforcement culture.

- **Issue: Accelerating responses of law enforcement agencies** – The definition of cybercrime varies from country to country. Countries need to have a universal consensus on what constitutes as cybercrime. Prosecution of cybercrime activities is

also a challenge due to the differences in legislation and jurisdiction of countries. Global agencies such as Interpol and countries can help shape discussions on this by building more awareness and understanding of cybercrime operations.

- **Issue: New paradigm across countries** – Law enforcement agencies should set out to define the constitution of 'public interest' in cybercrime investigations. For instance, the police may intervene in the event a particular category of online scams become pervasive to the public. One noticeable trend involves the exploitation of the relative reluctance or weakness of the courts to prosecute cybercrimes which occur in a multi-jurisdictional situation.

- **Issue: Legal frameworks against cybercrimes** – Some parties sell or use tools that are not illegal in themselves. An example would be Shadowbroker which rents and leases tools that assist cybercriminals to carry out their attacks. In many countries, existing legal structures would not be adequate to prosecute Shadowbroker. Countries need to develop their legal frameworks to criminalize such activities.

- **Issue: Adoption of open-source cybercrime technology tools** – Enabling technological tools to remain open-source on platforms such as GitHub allows professional coders to critically analyse for flaws and improvements. To encourage the adoption of open-sourced technology tools by digital forensic experts, it is important for experts and practitioners to verify if the tools are operationally and forensically sound to be utilised and applied across whole of industry.

- **Issue: Role of AI in cybercrimes** – An Artificial Intelligence (AI) system is one which is fully autonomous which can be programmed to perform functions on its own through machine learning. Though AI can aid cybercrimes, the legal presence of an AI in court is still not a viable option as physical evidence is required in court. Therefore, agencies like the Interpol must continue building better collaboration and connections between the law enforcement agencies in different countries to collecting and analysing cyber evidence obtained.

Distillation

- A comprehensive spectrum of tools, ranging from open-source information on social media to artificial intelligence, can be used to effectively tackle cybercrimes.

- Collaborations with other countries can contribute to a mature legal framework.

- Law enforcement agencies must adapt and be more agile in responding to the ever-changing nature of cybercrimes.

Panel 3: Psychology of Cybercrime

Inside the Mind of Cyber Criminals: A Look into the Dark Web
Andrei Barysevich, Director of Advanced Collection, Recorded Future

Cybercriminals have a romanticised, "larger than life" misperception surrounding them, leading to the growth of their communities. The reality is that they are common criminals who can be captured through good police techniques.

- The Dark Web contains the ecosystem of the criminal underground. In order for law enforcement to get into the system, they need to infiltrate criminal communities and forums, befriend perpetrators, and then arrest them.
- The online space is made up of the (i) Surface Web; where most public information is available, (ii) Deep Web; which contains secure servers and confidential information, and (iii) Dark Web; which contains encrypted sites and anonymous & illegal activity.
- Some cybercriminals involved in fraudulent activities have been caught by law enforcement because they exposed themselves on social media or boasted about themselves online – as they tend to have a desire for fame and recognition. However, legislation against cybercrime is still weak in many countries, resulting in them not being prosecuted as vigorously as regular criminals.
- The most common cybercrimes on the dark web include fraudulent bank accounts, stolen credit cards, and compromised credentials of individuals and businesses. Cybercrime itself is essentially a business, which requires start-up capital and reputation to succeed. The most successful attacks are perpetrated by syndicates made up of people from a variety of professions.
- Approximately 200,000 events occur on the Dark Web daily, with incidents increasingly happening in Asia and South America. There is a strong demand for APAC bank accounts.
- The future of combating cybercrime on the dark web has to involve a symbiosis of manual research and technology. There is a need for real humans to make final decisions; reliance only on technology may be counterproductive.

Interpersonal Cyber Crime Victimisation: Findings of a Survey in Eight Indian Cities
K. Jaishankar, Head, Department of Criminology, Raksha Shakti University (Police and Internal Security University), India

Interpersonal cybercrime victimization is on the rise in India, and the anonymous nature of cyberspace blurs the lines between perpetrators and victims, and the very definitions of cybercrime.

- The targets of cyber-attacks today are not only machines, but include humans and their emotions. 'Real human attacks' are becoming increasingly common in the form

of cyber bullying, cyber violence, cyber stalking, cyber pornography, and cyber deceptions/thefts.

- In India, the patriarchal structure of society has infiltrated cyberspace where women continue to be the main victims of online abuse and harassment. In this society, it is a great challenge to get victims to step forward and volunteer as respondents of such surveys.

- The survey results indicate that the most common reasons for victimisation are for vengeance, jealousy, and emotional outrage. Perpetrators tend to be ex-boyfriends or girlfriends, friends, or complete strangers.

- Awareness on privacy rights and legal issues surrounding cybercrimes is higher in cities like Bangalore, and lower in Delhi and Chennai, indicating that the level of cybercrime is not connected to how developed the city is, but on other societal factors.

- Monetary loss was one of the significant crimes faced by the respondents (mostly males). Cyber bullying on social networking sites was the most prevalent crime.

- Regulation of the internet may be required. As the Internet was invented and is managed largely by the West, there needs to be a "decolonization" of the internet, such that values and norms respectful of the culture of a society can be adapted into the legal infrastructure of cybercrime. A behavior of reporting cybercrimes needs to be better inculcated.

Psychology of Ransomware

Penelope Wang, Psychologist, Crime, Investigation and Forensic Psychology Branch, Home Team Behavioural Science Centre, Home Team Academy, Singapore

Perpetrators of ransomware employ psychological tactics to manipulate their victims. The threats of ransomware can be mitigated by promoting optimal cyber hygiene levels.

- Ransomware is one of the world's leading cyber threats, which is expected to become a billion-dollar criminal industry in the near future. In quarter 1 of 2016 alone, cybercriminals made US$209 million off ransomware.

- The most recent ransomware attacks which affected countries around the world were the "WannaCry" in May 2017 and then "NotPetya" in June 2017. Victims included NHS in the UK, MegaFon in Russia, FedEx in the USA and Renault in France. Perpetrators of such ransomware attacks are interested in not just ransom, but destruction and disruption of their targets.

- According to the psychology of ransomware, there are 3 parts to analysing why perpetrators are successful and why victims succumb to paying up: (i) Distribution; studying how the ransomware gains access to the system through exploiting victim's vulnerabilities, (ii) Demand; focuses on victims' reactions to the ransomware demand, and (iii) Payment; looks into how perpetrator's frame their message to coerce victims to pay up quickly.

- The distribution of ransomware primarily through social engineering, or phishing, is done by manipulating people to obtain their confidential information or perform certain actions that facilitate infiltration into secured systems. It is easier to exploit natural human inclinations to trust others than to find methods of hacking secure devices.

- How victims react to ransomware determines its success. There is no guarantee that victims will get their data back even if they pay up; it is recommended that they do not pay the ransom and report the incident to relevant authorities. However, individuals and businesses continue to pay large sums of money in ransom with the hope of retrieving confidential files.

- The primary psychological reasons that victims pay the ransoms are out of grief and fear. Grief is divided into 3 dimensions – avoidance, encounter, and reconciliation – such that a victim's ability to think is impaired and in order to minimise negative emotions, he/she pays up. Fear, viewed from an evolutionary perspective, prioritises speed over accuracy in decision-making such that when confronted with a threat victims tend to respond quickly in order to overcome the fear. According to Appraisal Tendency Theory, fear leads to a greater perceived lack of control, after which victims become pessimistic and make risk-averse choices such as paying a ransom.

- To improve cyber hygiene in Singapore and mitigate the ransomware payments, it is recommended that the gap is bridged between awareness and behaviour through education and removing barriers to implementation for different groups. Furthermore, cyber security partnerships should be promoted between the public and private sectors, and the wider international community. Finally, there must be emphasis on creating a culture of cyber resilience, such that victims respond adequately and competently to cyber threats. System hardening, incident exposure, and red teaming exercises should also be included in a resilience framework.

Syndicate Discussions

- **Issue: Ethical and human rights considerations during investigations** – Monitoring the activities of cyber criminals could lead to useful insights of criminal intent and provide law enforcement to identify opportunities to strike at the appropriate moment. However, ethical and human rights have to be considered alongside legal implications of setting online baits/traps for cybercriminals and avoid entrapment.

- **Issue: Psychology of a hacker** – The number of participants in the dark web has increased to over 500,000 participants (estimated) today. The established criminals eventually start seeking attention to feel acknowledged and that people recognize them. Cybercrime is a business and investment for them that enables them to feel monetarily satisfied. Eventually, they seek out recognition and acceptance into private high-profile social circles. After a while, if they go on undetected, they start to feel invisible and consider themselves, in a complacent way, smarter than the rest. At this point, they may expose themselves.

- **Issue: Internet separation** - Efforts such as Singapore's Internet separation initiative can help minimise the impacts from cyber-attacks. The inconvenience is worth it because there are many organisations that had been breached and criminals were able to easily conduct more lateral attacks with the data obtained; this would not be possible if networks were segregated.

- **Issue: Lack of awareness among web users** – It is difficult to convince the public to take simple steps to improve their online hygiene, such as using strong passwords, or subscribing to password managing programs and apps. People are afraid of these password management companies getting hacked, but in the unlikely event that heavily protected sites are breached there is very little chance of one's details being picked out of the potentially hundreds of millions of customers. The issue is also generational; older users are often more vulnerable from their lack of awareness.

- **Issue: Increasing public awareness of dangers of paying in ransomware cases** – Messages could be framed to emphasise the fact that payment to cybercriminals would further perpetuate the vicious cycle of ransomware activity. Highlighting the avenues victims could turn to (e.g. Cybersecurity Agency of Singapore) to recover stolen data can reduce the likelihood of payment to criminals and can help alleviate the distress of victims.

- **Issue: Streamlining reporting processes for cybercrime victims** –Victims should be encouraged to come forward and share details of ransomware attacks to relevant authorities. Enabling simpler reporting functions will reduce the complexity for victims. For instance, Europol's public access online forms enable a simple and streamlined reporting system for victims to share details on their ransomware attacks with law enforcement.

- **Issue: Cyber resilience, cyber security and cyber hygiene in Singapore** – Cyber resilience acknowledges that cybercrime can happen to anyone, so we must prepare for recovery. Cybercriminals often profile their targets, selecting the most vulnerable individuals e.g. those who will be most affected by data loss. As such, regular 'red teaming' exercises (simulated attacks) can help to inoculate individuals with better emotional management to prevent victimisation. Especially for large organisations, it is important to go through the experience of an attack to see how the organisation copes with the attack and responds to it, forcing employees to make decisions and think about why they made those decisions. This helps employees stay more prepared psychologically. Singapore is improving in terms of cyber hygiene, but more needs to be done. People may know what they need to do but may not do it. Studying the effectiveness of cyber security awareness campaigns is an area that requires more research.

- **Issue: Collaboration between states and nefarious online actors** – Some states (e.g. United States) arrest hackers and give them the option of working for the state as an alternative to serving prison time. In other states (e.g. Russia), state security agencies even pay criminals for their efforts. For example, in 2016 two FSB officers were arrested after being caught manipulating hackers from the global hacktivist network, Anonymous.

Distillation

- Detailed study and analysis on the psychology of cybercriminals can provide valuable insights on the motivations, modus operandi and weaknesses.
- The evaluation of existing public campaigns to identify areas in which cyber hygiene can assist in refining messages which do not resonate/are unclear to the public.
- Regular red teaming exercises can help to inoculate the public to better respond in the event cybercrime occurs.

Panel 4: Case Studies in Cybercrime

Europol's Experience in Tackling Cybercrime
Benoit Godart, Head, EUROPOL Office, INTERPOL Global Complex for Innovation

Europol plays a big role in combating the different areas of cybercrime. Collective action from international organisations, law enforcement agencies, and the private sector is needed to fight cybercrime.

- The cybercrimes that Europol investigates include ransomware, large scale DDOS attacks, child sex exploitation online, payment fraud, and use of online criminal markets.
- Cybercrimes can be perpetrated by a variety of actors, including insiders, hacktivists, cyber criminals, and state actors, There is a need for heightened cooperation between law enforcement agencies to combat these actors. One example given was cooperation with the United States' FBI in bringing down the Silk Road, an online marketplace for illicit material.
- Europol coordinates 73 law enforcement agencies in 28 member states. Its main responsibilities are in strategy and operations, working closely with the private sector, academia, and national CERTs (Computer Emergency Response Teams).
- There are different philosophies between Europol and CERTs. The goal of law enforcement is to gather evidence, while the job of CERTs is to speedily restore systems, which makes investigative work difficult.

A Global Corporation's Perspective on Dealing with Cybercrime and Cyberattacks
Goh Seow Hiong, Executive Director, Global Policy & Government Affairs, Asia Pacific, Cisco Systems

Large cybersecurity firms like Cisco place their priority on defending and remediating a cybersecurity incident rather than to preserve evidence for investigative purposes.

- Cisco uses 'red teams' to detect vulnerabilities. While under the same leadership as the threat detection team, this red team is deliberately kept separate and given a free rein to attack systems within the ambit of the law.
- The biggest problem facing corporations is not knowing when they have been compromised. On average, corporations took 100 to 200 days to detect malware in their systems.
- To address the lag in detection, there are three processes a corporation need to improve on. First, they need insight into their own systems. This allows corporations to prevent damage, quarantine malware quickly, and allows investigation into potential malware. Second, they need to integrate the cybersecurity products they use. These products need to be able to share interfaces and threat information.

Third, they need to innovate processes to improve the visibility of threats and reduce the time needed to detect malware.

Cybercrime Case Studies in Malaysia

Mohd Zabri Adil bin Talib, Head of Digital Forensics, Cyber Security Malaysia

The speaker shared Malaysia's experience dealing with cybercrime, specifically a case involving cyber forensics into Android malware.

- The malware appeared to be a banking app that was installed on a victim's phone. The website used to deliver the malware tricked victims by looking similar to the bank's legitimate website, allowing credentials entered in the fake website to be phished.
- There were three main challenges in solving the case. First, there were problems taking down the fake websites because the website servers were in Ukraine and Russia, and the law enforcement agencies there were not cooperative. Second, because of the cross border issue, Malaysian police were unable to act directly on the case. Third, because it was the transactions appeared to have been authorized by users' valid credentials, the banks were able to deny liability.
- To avoid a repeat of such incidents, there is a need for more awareness programmes and malware remediation. A knowledge sharing platform should be set up to quickly deal with malware.

Capturing Child Sex Offenders on the Dark Web

Graham Pease, Detective Senior Constable, Task Force ARGOS, Queensland Police Service

Police investigations online still revolve mainly around detective work.

- Pease detailed the work done by Task Force Argos does in capturing child sex offenders on the Dark Web, by operating a child pornography ring. He described how a major child sex offender was captured in Australia with cooperation from counterparts from Europol and Denmark.
- Pease attributed the success of Task Force Argos to the legislation that allowed them to operate outside the bounds of the law, albeit with strict conditions. Instead of taking down the child sex ring, Task Force Argos was able to run the ring for a fixed period of time to capture the criminals who were producing content in the ring.
- While technological solutions were a good to have if police forces could afford it, the key to a successful investigation was good old fashioned investigative and undercover work. Partnerships with other law enforcement agencies are also an important part in bringing down the child sex ring, especially with suspects in other jurisdictions.

Syndicate Discussions

- **Issue: Motivations of cyber criminals for data theft** – The adage "Data is Gold" holds true for cybercriminals due to the opportunities stolen data can provide. Data can be sold on the Dark Web by professional hackers. Other categories of data coveted by professional hacking syndicates include government secrets and private intellectual property for espionage purposes.

- **Issue: Developing regulations to cope with growing challenges** – An ASEAN charter of law enforcement agencies, similar to Europol, could be set up. The inclusion of ASEAN countries in the Budapest Convention would be one step forward to aligning international efforts of countries to tackle growing cyber challenges. The Convention also allows for significant flexibility, owing to the dynamism of the threats posed by cybercrime.

- **Issue: Utilising expertise of Singapore's private sector** – Singapore's private sector has much to contribute in terms of technological expertise. However, small and medium scale enterprises lack the technological capabilities and resources to secure their business against cyberattacks. Government efforts could look into lowering the costs for businesses in securing critical infrastructure for business operations.

- **Issue: Eastern Europe as an epicentre of cybercrime** – Approximately 80% of cyberattacks affecting the European Union is conducted by Russian-speaking organised crime groups. To counter this specific threat Europol hires analysts proficient in the Russian language and the unique jargon used in the relevant forums. Europol also has an operational agreement with Interpol to share resources and conduct investigations outside of the EU.

- **Issue: Cooperation between private companies and state law enforcement agencies** – The major is issue is the building of trust. In the past almost no data was shared between the private sector and police, but considerable ground has been made in recent years and relationships are improving. The key is to focus on mutual benefits and how effective coordination can meet the particular interests of each party.

- **Issue: The role of community policing for child abuse** – The community can try to influence local government representatives to enable policy changes for the greater protection of children, for instance, by ensuring adequate legislation for the prosecution of perpetrators. Collaboration with the private sector is equally crucial as the technical expertise, knowledge and skillsets could prove greatly beneficial to law enforcement agencies.

- **Issue: The infiltration of child sex offender groups on the dark net** – Forum membership requires one to upload images of child exploitation, which police are permitted to do in certain jurisdictions. The psychological effects on people dealing with such material can be significant, but it is a last resort strategy and often the only way of gathering information to identify the offenders.

- **Issue: Raising public awareness of cybercrime** – The media can play a role to increase knowledge and practice of online hygiene among the general public. In Malaysia, authorities run hacking competitions and debates in schools, which serve both to promote understanding among young people and their parents, and to instil a sense that 'white-hat' hacking to protect the nation can be 'cool'.

- **Issue: Securing Internet of Things (IoT) devices** – The increasing proliferation of smart devices provides significant opportunities for cybercriminals to compromise these devices (e.g. attacks can range from hacking to denial of service attacks). As such, governments and technology companies should define the standards of security of smart devices. Regulatory controls on smart devices can help ensure the safety and security of consumers.

Distillation

- Improving collaboration and trust between law enforcement, local communities and the private sector can provide comprehensive approaches towards dealing with cybercrime.

- Inter-agency discussions and sharing of best practices (e.g. between Interpol and Europol) synergises investigative resources and conduct multi-jurisdictional investigations abroad.

Closing Panel/Moderated Discussion

The CENS Cybercrime workshop concluded with discussion on possible reasons for cybercrime and the need for further research, collaboration and raising public awareness towards better understanding of cybercrime.

- The workshop discussed possible reasons for cybercrime. Cybercrime has been understood mainly from the technical and economic perspectives. Cybercrime's exploitation of vulnerabilities in human behaviour is an emerging perspective that deserves future exploration through multidisciplinary research in the areas of psychology and social sciences.

- The internet represents a low barrier to entry for cybercriminals due to its affordability and provision for anonymity. Therefore, the technical community needs to build investigative skills and think out-of-the-box to keep up with the dynamic operating landscape of cybercrime.

- Cooperation is integral to the resolution of cybercrime. Partnerships and international forums therefore play an important role in combating the challenges of cybercrime. Cooperation can take place between a variety of stakeholders: law enforcement, CERTs, and the private sector

- The proliferation of Internet-of-Things (IoT) devices will also contribute to cybercrime in future. It is therefore imperative to think about the implications of smart devices on cybercrime and design ways to protect users. .

- Public awareness should be conducted to better educate the public against the dangers of cybercrime. There is also the need to bridge the gap between awareness and behaviour so that tackling cybercrime becomes a shared responsibility between the government and citizens.

Workshop Programme

Venue: Marina Mandarin Singapore
Taurus & Leo Ballroom, Level 1 (unless otherwise stated)

Monday 13 November 2017

0800–0850hrs **Registration**

Venue : Taurus & Leo Ballrooms Foyer, Level 1

0850–0900hrs **Workshop Welcome Remarks** by ***Shashi Jayakumar****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

0900–1000hrs **Panel 1: Overview of Global Cybercrime**

Chair : ***Shashi Jayakumar****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Global Cooperation in Fighting Cybercrime** by ***Zachary Delecki****, Assistant Legal Attache, Federal Bureau of Investigation, US Embassy Singapore*

Mutual Legal Assistance to Combat Transnational Cybercrime by ***Adam Palmer****, Vice-President, Financial Services Roundtable*

Driving Cyber Security Policy Insights from Information on the Internet by ***Qiu-Hong Wang****, Assistant Professor, School of Information Systems, Singapore Management University*

1000–1115hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1115–1130hrs **Networking Break**

Venue : MMB Foyer, Level 1

1130–1230hrs **Panel 2: Cybercrime and the Dark Web**

Chair : ***Norman Vasu****, Deputy Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Cybercrime Investigations in The Dark Web** by ***Vitaly Kamluk,*** *Director, Global Research & Analysis Team, APAC, Kaspersky Lab*

Taking a Walk in The Dark Web by ***Vicky Ray****, Director, Palo Alto Networks*

Digital Forensics in Cybercrime *by* ***Christopher Church,*** *Senior Mobile Forensics Specialist, INTERPOL Global Complex for Innovation*

1230–1330hrs **Lunch**

Venue : MMB Foyer, Level 1

1330–1445hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces Ballrooms, Level 1

1445–1545hrs **Panel 3: Psychology of Cybercrime**

Chair : ***Terri-Anne Teo****, Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Inside the Mind of Cyber Criminals** by ***Andrei Barysevich****, Director of Advanced Collection, Recorded Future*

Interpersonal Cyber Crime Victimization: Findings of a Survey in Eight Indian Cities by ***K Jaishankar****, Head, Department of Criminology, Raksha Shakti University (Police and Internal Security University), India*

Psychology of Ransomware by ***Penelope Wang****, Psychologist, Crime, Investigation and Forensic Psychology Branch, Home Team Behavioural Science Centre, Home Team Academy*

1545–1600hrs **Networking Break**

Venue: MMB Foyer, Level 1

1600–1715hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1715hrs **End of Day 1**

1800–2030hrs **Workshop Dinner (By Invitation Only)**

Venue : Aquamarine, Level 4

Tuesday, 14 November 2017

0800–0900hrs **Registration**

Venue : Taurus & Leo Ballrooms Foyer, Level 1

0900–1020hrs **Panel 4: Case Studies in Cybercrime**

Chair : ***Benjamin Ang****, Senior Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Europol's Experience in Tackling Cybercrime** by ***Benoit Godart****, Europol Liaison Officer, INTERPOL Global Complex for Innovation*

A Global Corporation's Perspective on Dealing with Cybercrime and Cyberattacks by ***Seow Hiong Goh****, Executive Director, Global Policy & Government Affairs, Asia Pacific, Cisco Systems*

Cybercrime Case Studies in Malaysia by ***Mohd Zabri Adil Bin Talib****, Head of Digital Forensics, Cyber Security Malaysia, Malaysia*

Capturing Child Sex Offenders on the Dark Web *by* ***Graham Pease,*** *Detective Senior Constable, Task Force ARGOS, Queensland Police Service*

1020–1035hrs **Networking Break**

Venue : MMB Foyer, Level 1

1035–1150hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces Ballroom, Level 1

Syndicate 4

Venue : Aquarius Ballroom, Level 1

1150–1235hrs **Closing Panel / Moderated Discussion**

For this session, all participants and speakers will be able to discuss as a group some of the key issues and takeaways uncovered during the course of the Workshop

Chair : ***Shashi Jayakumar****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

1235–1400hrs **Closing Lunch**

Venue : MMB Foyer, Level 1

1400hrs **End of Day 2**

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information about CENS, please visit www.rsis.edu.sg/research/cens/.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg.

About the National Security Coordination Secretariat

The **National Security Coordination Secretariat (NSCS)** was formed under the Prime Minister's Office in July 2004 to coordinate security policy, manage national security projects, provide strategic analysis of terrorism and national security related issues, as well as perform Whole-Of-Government research and sense-making in resilience.

NSCS comprises three centres: the National Security Coordination Centre (NSCC), the National Security Research Centre (NSRC) and the Resilience Policy and Research Centre (RPRC).

Please visit www.nscs.gov.sg for more information.