CYBERSECURITY: EMERGING ISSUES, TRENDS, TECHNOLOGIES AND THREATS IN 2015 AND BEYOND

Edited Volume
March 2016

Edited by
Caitriona Heinl and Eugene EG Tan

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

Cybersecurity
Emerging Issues, Trends, Technologies and Threats in 2015 and Beyond

Edited by:
Caitriona Heinl and Eugene EG Tan
Centre of Excellence for National Security (CENS)

Foreword

This collection of short commentaries presents views on many of the on-going debates relating to cybersecurity policy. The authors include government practitioners and leading academics who addressed the Centre of Excellence for National Security workshop on "*Cybersecurity: Emerging Issues, Trends, Technologies and Threats in 2015 and Beyond"* on 20-21 July 2015. The workshop focused on the possible implications of these debates on countries like Singapore and the wider Southeast Asia/Asia Pacific region, particularly in terms of the regulatory, operational and governance domains. The quality of contributions at the workshop led to the decision to publish them here. These edited commentaries which are based on the workshop presentations have been expanded to provide greater depth to those arguments originally made in the presentations.

Table of Contents

A New Cybersecurity Paradigm 3
Daniel Castro, Vice President, Information Technology & Innovation Foundation

Should We Rein in the Powers of the State by Restricting its Surveillance Powers, or Do Some of our Own Monitoring by Expanding Those Powers Still Further? 11
Simon Chesterman, Dean, Faculty of Law, National University of Singapore

Balancing National Security Needs with Data Privacy and Freedom of Expression Concerns: Singapore's Perspective 19
Bryan Tan, Partner, Pinsent Masons MPillay LLP, Singapore

Securing Singapore's Smart City From Emerging Cyber Threats 27
Michael Mylrea, Manager for Cybersecurity and Energy Infrastructure, Pacific Northwest National Laboratory. National Science Foundation: Executive Cyber Security Doctoral Fellow, George Washington University

Challenges and Opportunities for Better Communication, Cooperation and Collaboration in International Cybersecurity in Asia 33
Yono Reksoprodjo, Lecturer and Researcher on Asymmetric Strategy Studies, Indonesia Defense University – (UNHAN)

Global Implications of the United States – China Cyber Relationship 39
Jason Healey, Senior Research Scholar, Columbia University's School of International and Public Affairs

Cyber Relations between the United States and China: A Chinese Perspective 47
Zhu Qichao, Director and Professor of the Center for National Security and Strategic Studies (CNSSS), National University of Defense Technology, China

Lethal Autonomous and Cyber Weapons – Do They Challenge International Humanitarian Law? 57
William H Boothby, Air Commodore (Retired)

Technology, Threats and Trust in an Interconnected World 67
Robert J. Butler, Senior Advisor to The Chertoff Group

The European Union's Approach to Cybersecurity and Defence 73
Wolfgang Röhrig, Programme Manager, Cyber Defence at the European Defence Agency

Cybersecurity and Cybercrime: Philippine Perspectives and Strategies 89
Geronimo L. Sy, Assistant Secretary and Head, Office of Cybercrime, Department of Justice

Cybersecurity Trends and Issues: A Singapore Perspective 99
John Yong, Director, Infocomm Security Group, Infocomm Development Authority of Singapore

Contributors' Biographies 107

About CENS, RSIS, and NSCS 117

A New Cybersecurity Paradigm

A New Cybersecurity Paradigm

Daniel Castro, Vice President, Information Technology & Innovation Foundation

Around the world, cybersecurity has taken on a new urgency as the digital economy has matured over the past decade, and businesses and consumers are more reliant than ever on information systems. Moreover, the importance of cybersecurity continues to grow each day with the emergence of a new wave of cyber-physical systems that make up the Internet of Things including wearables, "smart" devices for the home, autonomous vehicles, and unmanned aerial systems (also known as drones). Yet against this backdrop of digital transformation, it is increasingly clear that both the public and private sector are failing to keep pace with cybersecurity threats.

To address this pervasive problem, governments around the world need to fundamentally realign their cybersecurity efforts to address this new reality.

The problem

The failure of today's approach to addressing cybersecurity is evident in the news headlines. Within the past year, numerous businesses around the world have fallen victim to both state and non-state hackers including well-known companies such as Target, Sony, and HSBC, resulting in millions of records about consumers being exposed.

Exposure to these attacks is partially the result of a market failure - companies are not investing sufficient resources in cybersecurity because they do not suffer all of the harmful consequences of a successful attack. As long as these negative externalities are not addressed, the private sector will spend less than it should on cybersecurity.

In addition, governments around the world have also failed to secure their systems. Most notably, the U.S. government has not been immune to these threats. Last year, the Office of Personnel Management revealed it had been victim of one of the most extensive cyber attacks in U.S. government history in which hackers obtained the sensitive information of 22.1 million federal employees, contractors, and their friends and families. The OPM attack was successful because the agency had poor cybersecurity practices, but this attack could have been prevented. This hack is a public management failure that has resulted from the U.S. government becoming apathetic towards cybersecurity and tolerating poor performance. As long as senior government leaders are not held accountable for cybersecurity vulnerabilities, this culture of indifference will continue unabated.

The obstacles

Unfortunately some of the major government efforts to improve cybersecurity have been misguided. First, national security interests often trump economic considerations. In the United States, this dynamic has played out in both the intelligence community's decision to engage in widespread surveillance and the on-going debate over strong encryption. In both cases the intelligence community and law enforcement have argued for actions that have jeopardised the economic interests of the nation. For example, the Snowden documents revealed that the NSA likely weakened cryptographic standards in an effort to enable more surveillance.

The NSA's excessive surveillance practices, while possibly providing important intelligence on the threats from cyber attacks, have likely cost U.S. businesses more than $35 billion as numerous foreign buyers of U.S. technology have turned elsewhere for products and services because they fear that buying from a U.S. company exposes them to unnecessary risk. The net result has been less overall security and serious economic consequences for the U.S. tech sector.

More recently, the Director of the Federal Bureau of Investigation, among other senior government officials, has argued that U.S. companies should not be using strong encryption that does not include a backdoor to allow government access. If such a policy were to be adopted, it would not only leave consumers less secure, but it would send foreign buyers of U.S. technology to other overseas providers. This same debate over encryption is playing out in other countries as well, with the economic considerations often taking a secondary level of importance.

Second, where economics interests have played a role in decisions about cybersecurity, it has often been to support protectionist policies. Some countries have incorrectly argued that the only way to ensure good security is to produce products and services domestically, or undergo domestic security reviews. In addition, a number of countries have begun considering or implementing data localisation policies that require data to stay within a country's borders or be processed domestically.

There are many examples of these anticompetitive policies such as China's removal of many foreign businesses from its Central Government Procurement Center's list, India's Internet of Things strategy which puts companies making smart devices on its Preferred Market Access list, and Russia's data localisation requirements. In fact, the best way to secure data is not to keep it local but to store it on the most secure systems. Unfortunately, all of these policies have the net impact of making it more difficult for the public and private sector to access the more secure technology by raising the cost of imported information technology products and services, reducing competition, and locking out foreign producers.

The solution

The basic assumption of most governments is that they are best positioned if their systems are secure, but everyone else's systems are penetrable. For example, if an intelligence agency discovers a new vulnerability, it may

choose to not disclose this information so that it can exploit the weakness. This mindset has led to policies that do little to disrupt the obvious cybersecurity failings in industry and government and discourages cooperation. Rather than continuing with this adversarial approach, all nations should look at cybersecurity as a communal goal, like global peace, that everyone benefits from. With that in mind, nations should come together to work collaboratively on cybersecurity and endorse the position that the role of government should be to strengthen, not weaken, cybersecurity. This collaboration should involve joint investment in finding solutions to common cybersecurity problems and better cooperation between law enforcement to enable cross-border investigations of cybercrime. No nation should be allowed to become a safe haven for hackers without international repercussions.

In particular, governments should be focused on a dual pronged approach of improving both defensive capabilities and resiliency. On the defensive side, governments should be focused on hardening systems to lower the risk of a successful attack. In particular, governments should be working with the private sector to identify instances where organisations are failing to take the protective measures they should and ensure these measures are taken. Just as companies cannot operate in violation of a fire code or worker safety laws, neither should they be operating with known security problems.

On the resiliency side, governments should help develop better capabilities at reducing mistakes that arise from changes made to complex information systems. A number of recent high-profile computer systems and networks failures, such as at the New York Stock Exchange and United Airlines, were not the result of cyber attacks, but rather were the result of insufficient resiliency in highly complex systems.

The goal of government intervention should be to make it easy, cheap, and desirable for the private sector to do cybersecurity well. Moreover, given the market failures discussed previously, governments cannot entrust cybersecurity exclusively to the private sector. For example, government agencies should provide funding for cybersecurity research to address

underinvestment in this area by the private sector. Government agencies should also take an active role in assisting the private sector in improving its cybersecurity efforts, such as by having government-funded researchers work closely with the private sector to identify and eliminate threats. Government agencies should also share their knowledge about best practices with the private sector, especially for small businesses which may not have the cybersecurity expertise of larger organisations. For example, government agencies can release their own security assessments of the IT service providers and products they use, so that others can leverage this knowledge when making purchasing decisions.

Regulators can also play a greater role in promoting cybersecurity innovation. In particular, enforcement actions should use penalties to ensure that companies have an incentive to protect consumers from harm. For example, a company that suffers a data breach but has taken steps to encrypt customer data so that no personally identifiable information is exposed would not suffer a penalty whereas a company that did not take this step to protect its customers would face one. The goal with regulatory policy should be to shift company resources so that they are not merely trying to meet a compliance threshold, but rather are actually making consumers better off.

Finally, we need structural change in how governments develop cybersecurity policy. Senior government officials need to stop ignoring the economic consequences of cybersecurity policy decisions. Bringing the business community and trade policy specialists into cybersecurity policy decisions will provide a more balanced debate so that decisions are not made that put the needs of law enforcement and the intelligence community above all others or that allow protectionist policies to stand unchallenged.

For example, policymakers need to create rules for a well-functioning global market for IT that encourages countries to come together to establish a common hardware and software certification process. Achieving this will require setting up strong accountability measures and creating strong mechanisms to discourage cheating. For example, countries could agree to

international, rather than national, security testing standards and establish a principle that if a company's products are later discovered to have backdoors in it, then this company will be blacklisted.

Conclusion

In short, addressing the cybersecurity threats of tomorrow will require a fundamental realignment of how government has approached this problem until now, as well as strong leadership to overcome existing market and government failures and navigate the barriers that have impeded progress in the past.

Given the importance of cybersecurity to the digital economy, countries should come together to face these challenges and create a new paradigm for building secure and resilient systems.

Should We Rein in the Powers of the State by Restricting its Surveillance Powers, or Do Some of our Own Monitoring by Expanding Those Powers Still Further?

Should We Rein in the Powers of the State by Restricting its Surveillance Powers, or Do Some of our Own Monitoring by Expanding Those Powers Still Further?[1]

Simon Chesterman, Dean, Faculty of Law, National University of Singapore

In early 2015, it was announced that officers from Singapore's Bukit Merah West Neighbourhood Police Centre (NPC) would begin trials of body-worn cameras. The aim is to have cameras in use at half a dozen NPCs in 2015 and island-wide by June 2016.

The cameras are worn visibly and have an indicator that shows when they are recording. Data cannot be downloaded without proper authorisation and, in the absence of an on-going investigation, will be deleted after 31 days. During the 2015 budget debate, Second Minister for Home Affairs S Iswaran memorably described the cameras as "light, compact and not too sinister-looking".

How do we evaluate the decision to use such devices?[2]

Under an on-going European Union project ("Surveille") that examines the ethical, legal, and practical issues involved in the use of surveillance technologies for the prevention, investigation and prosecution of terrorist activities and serious crime, two basic aims have been explored: 1) To map the surveillance technology that is currently being deployed in Europe and elsewhere; and 2) To assess the costs and benefits of using that technology. In essence, this project has aimed to get a picture of what is happening and why.

Neither is simple, but it turns out that the “what” is easier to answer than the “why”. Surveillance is now a multibillion dollar industry. Publicly available figures show tens of billions of dollars being spent annually on video surveillance and interception of emails, telephone calls, and other messages. Forbes magazine has predicted a tenfold growth in the IT security industry over the next ten years. Such investments represent a cost in terms of dollars as well as in terms of lost privacy, but how do we assess the asserted benefits?

Security vs liberty?

Unfortunately, this is not an area in which decisions are always rational. The debate is often framed as the need to balance a supposed tension between security and liberty. The problem is that, when framed like this, liberty — privacy in particular — always loses.

This is partly because the side of liberty is often reduced to platitudes. Soon after the September 11 attacks in the United States, for example, senators were debating the USA Patriot Act’s surveillance powers. One of the senators invoked a founding father: “As Ben Franklin once noted, ‘if we surrender our liberty in the name of security, we shall have neither.’” But he misquoted Franklin, who was more nuanced. What Franklin actually said was: “Those who would give up essential Liberty to purchase a little temporary Safety deserve neither Liberty nor Safety.”

The costs and the benefits of surveillance

It is hoped that debates within Europe and elsewhere about surveillance technology will be better informed by a matrix produced by the Surveille Project that quantifies the effectiveness, ethics, and legality of surveillance technology.

In terms of effectiveness, the matrix scores a given technology based on its ability to achieve its stated goal, cost, design features that limit intrusions to privacy, and overall excellence as demonstrated in the field. Ethical considerations go beyond the strict letter of the law and include the nature of the harm to be prevented, the reliability of evidence, and the imminence of the threat. The criterion of legality includes the justification for surveillance, the necessity of using intrusive methods if less intrusive methods are available, and the proportionality of the action relative to the harm to be prevented.

These factors are intended to help policy-makers engage in a genuine cost-benefit analysis that does not rely on vague concepts of liberty and security. The approach also recognises that liberty and security are not mutually exclusive. Some things that might seem to increase security in the short term — such as profiling certain classes of individuals — can actually create the problem they intend to address, as when profiled groups become more marginalised as a result of being targeted.

Two types of problem still linger, however. The first is that agents of the state, like everyone else, often suffer from cognitive biases. It is not hard to imagine how a bureaucrat, for example, when faced with a proposal to use an intrusive new technology against a severe but remote threat, might prefer to allow it. Would you prefer to be criticised for some vague intrusion on privacy rights, or for letting the next shoe-bomber on an airplane? For this reason, many such decisions are referred to judges in the hope that they will be more detached in their assessment. Secondly, even when the violation of rights is considered as a factor, the limitation of that violation to a certain class of persons means that the decision-maker — and often the majority of the public — do not worry that it will affect them directly. This could be seen, for example, in the American public's blasé attitude towards surveillance of potential terrorists — until Edward Snowden revealed that the American government had expanded that set to include almost everyone.

More surveillance, more accountability?

Moving forward, it seems unlikely that the surveillance technologies that have already been deployed will be removed. However, if the power of the state to watch over us cannot be reduced, there is an alternative approach to reining it in: increase that power further.

In the United States, for example, a series of police killings of unarmed black men over the past year have led to calls for greater oversight. After Michael Brown was killed in Ferguson, Missouri, in August 2014 there were disputed accounts as to the circumstances of his death. In December, President Obama sought funds to pay for more than 50,000 body-worn cameras to be used across the United States. And a US$20m pilot programme was announced by the new Attorney General in 2015.

The funding came three weeks after another man, 50-year-old Walter Scott, was filmed being shot in the back as he ran away from officer Michael Slager — who had pulled Scott over for a broken tail light. That video was taken by a passer-by on a handphone, but it led to widespread outrage and showed the potential benefit of more cameras. In the face of such evidence, the officer was sacked and charged with murder.

It is possible, then, that such technology can do more than serve the interests of the state in helping to keep the public safe. It can also play a role in ensuring that the powers of the state are exercised properly and with greater transparency. However this will only happen if there are safeguards to prevent selective use of that technology.

In Singapore, for example, greater use of cameras by police might have offered more clarity on controversial incidents such as the riots in Little India in December 2013, or the death of Dinesh Raman while in custody in September 2010.

If the body-worn cameras are successful, it might also lead to a reconsideration of video-recording statements to police. As MPs Hri Kumar and Sylvia Lim have both argued in Parliament, this could reduce the need for the courts to spend time evaluating whether statements by the accused and witnesses were accurately recorded — a particular concern given several high-profile cases in which defendants alleged that they were coerced by the police. In the absence of such recording, as Professor Ho Hock Lai explained in the Singapore Journal of Legal Studies, it is all the more important to strengthen the right of an accused to have access to a lawyer.

A further concern is ensuring that such surveillance devices are not misused by third parties. The security firm iPower recently warned that it had found the Conficker computer virus on police body cameras in Florida. The dangers of body cameras being infected with malware range from casting doubt on their veracity as evidence in criminal trials to the possible redirection of surveillance data to unauthorised individuals.

"Not Too Sinister"

When opening the new Police Operations Command Centre in early 2015, the Prime Minister of Singapore, Lee Hsien Loong, posted a photo of himself on Facebook holding one of the new body-worn cameras — "No more 'I say/ you say' disputes over what happened" he wrote, adding a smiley face emoji. The Prime Minister is right, of course. But as we prepare for the deployment of yet more surveillance technology, it will be important to ensure that those cameras keep an eye on the state as well as on us.

---

[1] This article draws heavily upon an article first published in the Straits Times on 6 May 2015 as "To Monitor Citizens and the Surveillance State".

[2] For the past four years, the author was an external adviser to a European Union project that examines the ethical, legal, and practical issues involved in the use of surveillance technologies for the prevention, investigation and prosecution of terrorist activities and serious crime. The key findings were presented at the European University Institute's State of the Union event in Florence, Italy in 2015. Entitled "Surveille", the author explains that this is not some attempt by a radical organisation to derail the surveillance state. On the contrary, the project takes

surveillance seriously and is intended to help analyse it like any other government policy. Nor is it an ivory tower enterprise by academics: one of the consortium partners is Merseyside Police Federation and there has been extensive outreach to other police and intelligence service personnel.

Balancing National Security Needs with Data Privacy and Freedom of Expression Concerns: Singapore's Perspective

Balancing National Security Needs with Data Privacy and Freedom of Expression Concerns: Singapore's Perspective

Bryan Tan, Partner, Pinsent Masons MPillay LLP, Singapore

National security developments in Singapore

The traditional conception of national security has changed in recent years. Traditionally, national security was focused on physical infrastructure and defending against specified enemies or combatants that are visible. However, the threats to national security have now changed rapidly because of the rapid evolution of technology.

The threats are no longer confined to just the physical realm, but also extend to the financial system as well as to networks that now maintain communications. There is also an emergence of "submarine" threats. Submarine threats refer to the planting of devices that remain hidden over a period of time before surfacing later to wreak havoc. Examples of submarine threats would be the Duku malware and the modus operandi for the February 2015 Carbanak malware attacks against banks globally. The significance is that the effect of the threat is now free from the constraints of time – and anything could be perceived as a "ticking time bomb".

The changing state of national security has also led to the introduction of the term "Critical Information Infrastructure" (CII). This refers to systems which are necessary for the delivery of essential services to the public in various key sectors. These sectors generally include energy, water, finance and banking, government, healthcare, information communications, security, emergency services, and transportation.

Cyber attacks on CII often occur with little warning and have tremendous potential for contagion. These cyber attacks can disrupt daily lives and

threaten a nation's security, economy, public health, and safety, possibly even bringing a country to a standstill. It is precisely because of this that CII are now increasingly becoming prime targets of cyber attacks.

The Singapore Computer Misuse and Cybersecurity Act

The Computer Misuse and Cybersecurity Act (CMCA) was first passed in 1993 and its primary objective was to curb hacking, unauthorised use, and unauthorised access activities. Then in 1998, amendments were made to the Act, which was then known as the Computer Misuse Act, to curb other activities such as unauthorised modification of computer material, interception of computer services, and to introduce the notion that certain computers will be considered protected computers. Most recently, in 2013, the cybersecurity portion was added to CMCA thus resulting in the change of the title. With the added objective of cybersecurity, CMCA then provided for measures to be taken to harden the security of certain CII such as specific servers and networks. Moreover, it includes provision for an even more drastic step - for the Government to take over the operation of the CII, if required.

The evolution of CMCA should be of no surprise. The rapid evolution of technology and the accompanying sophistication of cyber criminals has meant that the Act would have to be modified. The rapid evolution of technology and the sophistication of cyber actors cannot be overstated. In July 2010, Stuxnet, a sophisticated form of malware, was discovered and reportedly responsible for affecting 45,000 industrial computers worldwide. Many of these systems were integral to a country's critical infrastructures such as energy, water, and communication networks. The more recent emphasis on cybersecurity is therefore not surprising - the Government now has to take effective and timely measures to prevent, detect, and counter cyber attacks that may threaten the nation's security or national interests.

The approach to cybersecurity is no different to how other national security threats in the physical realm are dealt with. For example, if there is credible

intelligence of a potential terrorist threat to an aviation system, the authorities would immediately take pre-emptive steps to enhance security measures for the airports and the carriers in response to that threat. Likewise, in cyberspace proactive and pre-emptive action against a threat must be taken before such threat materialises to cause harm.

Data protection

A related development in Singapore is the development of its data protection framework. For many years leading up to 2012, Singapore addressed data protection issues with industry-specific legislation and regulation. However, in 2012, general data protection legislation was enacted in Singapore which introduced nationwide legislation that required organisations which collect personal data to undertake steps to protect that personal data.

The move for such legislation is important for two reasons. First, it signals the increasing importance of data, especially personal data, and the use of databases in this era. Organisations have been notified that their treatment of personal data would now be required to adhere to certain minimum standards. While this personal data legislation covers personal data only, the fact that personal data is often collected with other data now means a much more considered approach is required in the collection and ensuing usage and treatment of the data. Organisations are now required to consider how they collect, use, retain, and dispose of personal data.

Second, in a broader context, such treatment of personal data in databases also increases the awareness of data protection issues, specifically relating to breaches of security. This significantly helps cybersecurity efforts as vast amounts of collected data could represent attractive targets for cybercriminals. Since such databases could be maintained by several parties, it would only take the weakest link to be exploited to cause significant damage.

Freedom of expression

In Singapore, freedom of speech is subject to the right of Parliament to make laws to restrict such right. The Internal Security Act, Sedition Act, and the law of defamation qualify this right. Hence, freedom of speech is not an absolute right but is limited where such right infringes the rights of others. The reason for this arrangement is largely a historical one including the racial disturbances and foreign subversion that Singapore experienced in its early years of nation building.

In most cases, freedom of speech and national security are not incongruous concepts. The question that remains is whether curbs in the name of national security have a chilling effect on the freedom of speech wherein the fear of these curbs extend beyond the actual reach of the curbs. The laws in Singapore have existed for a long period of time, at least compared to its history of nationhood, and have served the country well. Organisations and individuals that possess an outlook similar to that of Wikileaks and Edward Snowden have not hitherto been present in Singapore. The question then becomes whether the emergence of players with this kind of outlook will bring about a further change in the law surrounding the freedom of speech.

The Southeast Asian experience

An analysis of issues relating to Singapore's cybersecurity is not complete without also identifying the issues that occur within the ASEAN context. Cybersecurity issues have indeed been taken up in ASEAN with the work program to implement the ASEAN plan of action to combat transnational crime in 2003 and the formation of the working group for cybercrime in 2013. The ASEAN Regional Forum (ARF) also set out in 2006 its Statement of Cooperation in fighting cyber attack and terrorist misuse of cyberspace. It acknowledged the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyberspace and encourages the formulation of such a framework so that

committed ASEAN countries will work together to fight cybercrime and deal with cybersecurity issues. The ARF Statement on Cooperation in Ensuring Cybersecurity in 2012 further sets the goal of intra-ASEAN cooperation in dealing with cybersecurity issues including practical cooperation on confidence building measures and fixed milestones for cooperation.

ASEAN cooperation is important because cybersecurity threats are multi-dimensional and borderless and because cybersecurity threats to a country may originate outside its borders. With ASEAN economies so closely interlinked, the need for cooperation is a given. Further, the CII discussed above are not just merely physical assets but assets which extend to other, and several, borders. For example, the submarine cable systems which are buried within the region and carry Internet traffic are now very important to our means of communications. ASEAN cooperation is also important because measures taken by a single country alone may be insufficient. For instance, Section 11 of the Singapore Computer Misuse and Cybersecurity Act provides for offences to have a territorial scope and provides that an act committed outside Singapore by a person of any nationality may have effects on Singapore.

Outlying issues

Looking forward, additional issues that Singapore and Southeast Asia will most likely face in the future include government access to encryption – where governments mandate different laws, regulations, and schemes by which they can have access to encrypted data or protected source code. While some of these regulations are phrased in terms of national security, there are questions from industry as to whether some of these measures might be either protectionist or have an economic agenda. A similar issue also extends to local requirements and regulations where certain classes or types of personal data would need to be physically stored in servers within jurisdictions.

Another near term concern is whether governments should operate their own data network. Economics aside, some governments like South Korea are considering and others like the UK and Canada are in fact already starting to build their own specific dedicated networks. The move away from commercially available networks to build a government-only network is seen as necessary in order to reduce reliance on commercial providers as well as to enhance cybersecurity. While this might be the case, questions over such moves include: a) whether there might then be an economic impact on commercial providers by the withdrawal of a key customer; and b) whether such withdrawal would in fact be helpful in removing elements of threat to the network by the presence of government traffic and through the capacity for non-government usage.

Impact of national security restrictions on innovation and the digital economy

Singapore is currently a mature, knowledge-based economy. The ability to create, acquire, disseminate, and apply knowledge is key to sustaining economic growth, especially since the global marketplace of products and services has become more technology and knowledge-intensive.

A failure to reach an acceptable balance between national security measures and innovation for the digital economy would have a detrimental effect on the economy, in turn diminishing national security. Economic strength to innovate is one of the key pillars of the national security agenda and the key to this balance is to be adaptable and prepared.

The Government has always been prepared in an ever-evolving scenario of cybersecurity threats and attempts to stay one, or more, steps ahead. In the event that a cyber attack does occur, the national security agencies would want to ensure that Singapore's CII are adaptable enough to withstand, at least initially, an onslaught of cyber attacks in order to survive and then

eventually counter such attacks. But for Singapore to face these challenges, national security imperatives have to be constantly balanced with the twin needs of remaining creative and ahead in the innovation stakes.

Securing Singapore's Smart City From Emerging Cyber Threats

Securing Singapore's Smart City From Emerging Cyber Threats

Michael Mylrea, Manager for Cybersecurity and Energy Infrastructure, Pacific Northwest National Laboratory. National Science Foundation: Executive Cyber Security Doctoral Fellow, George Washington University

As Singapore and other smart cities become increasingly connected to cyberspace their risk to cyber threats increase exponentially. Smart cities need to develop a cyber-smart workforce, technology, policies and new risk management solutions.

Singapore is a smart city-state success story at the forefront of a third industrial revolution. Today, the Internet of Things (IoT) increasingly interconnects Singapore's cyber and physical systems, sensors, controls and smart technology into the digital fabric that links society and critical infrastructures such as transportation, health, finance and defence. Singapore's infrastructure investment is expected to grow by 50 per cent to about S$30 billion by the end of the decade.

Cyber smart city: opportunity and challenge

The cyber smart city opportunity of new IoT-inspired products, services and markets could boost the GDP of the world's 20 largest economies by $14.2 trillion by 2030, according to a recent study by Accenture. This trend can be seen in Singapore's smart buildings, where converged information technology (IT) and operational technology (OT) platforms and devices integrate multiple electronic systems to support building management and business functions. Smart building technology is increasing energy efficiency and conservation of natural resources. Smart transportation is making cities more efficient. Smart health solutions are helping people live healthier lives and providing early warning against pandemics.

But the cyber smart city challenge is to secure all of these converged networks and devices from complex and evolving cyber threats. Hackers continue to exploit smart devices to steal, manipulate and disrupt cyber and physical systems. Cyber attacks have been used to infiltrate corporate networks through smart building controls, blow up furnaces in steel plants, and cause generators to fail. In 2013, Target, a large U.S. retailer, was hacked through its smart heating ventilation and cooling system, exposing corporate networks and over 40 million customer's credit cards. Similar vulnerabilities are prevalent in thousands of networked industrial controls systems.

A cyber-secure smart city will require a more holistic cybersecurity approach that fosters a culture of cybersecurity. Traditional information assurance solutions to risk management are vulnerable to IoT's expanded attack landscape: more networked devices exchanging larger data sets. Secondly, many industrial control systems need to be running 24/7, lack secure communication protocols and include legacy devices that are not interoperable or secure when combined with new IoT technology.

So what can Singapore do to realise the smart city opportunity and overcome the cybersecurity challenge?

Developing a cyber smart workforce is imperative. Even as some technical cybersecurity defences improve, humans remain the weakest link in cyberspace. A secure architecture requires a workforce to be continually trained in best cybersecurity policies, practices, and technology. A cyber smart city workforce must understand how to secure converged IT and OT environments.

Investments in human resource development should foster skills in science, technology, engineering and math as well as the social sciences such as human and organisational learning and behavioural psychology. The IT and OT cybersecurity skill set will be increasingly necessary to secure smart technology and systems, while the social sciences will help encourage

smart policies and processes that optimise the technology and help protect us from ourselves.

Cyber smart policies and solutions

Cyber smart policies and regulations are imperative for Singapore's continued success and survival. Cyber smart policies should help increase cybersecurity of critical infrastructures such as energy, finance, and telecommunications. Smart cities depend on these inter-related and symbiotic infrastructures for their economic livelihood, security and survival. Unfortunately, the increased networking and convergence of information communication technology and critical infrastructure has also increased the vulnerability to cyber threats.

Smart cities are fuelled by prodigious amounts of data that becomes more valuable as it is collected, aggregated and analysed. Big data needs to be protected by policies that curtail industrial espionage and strengthen intellectual property protection. One incentive for doing so is increased foreign direct investment. International corporations will increasingly move and expand in nations that protect intellectual property, encourage ingenuity and seek new ways to marry man and machine through education, not malware and hacking.

Cyber smart risk management solutions should provide a holistic defence in-depth approach to secure how data is being collected, shared and stored. Advanced intrusion detection systems and firewalls combined with encrypted data between servers, devices, sensors and enterprise networks are a good place to start. New security solutions for machine-to-machine secure communications are needed.

Technical solutions are only as strong as the risk management policies in place to respond to and prevent attacks. Secure standardisation of communication protocol in IoT can help facilitate more secure and interoperable smart cities.

Any effective cyber risk management solution should quickly adapt to the threat, helping to limit damage and assure continuity of operations.

The next 50 years

In considering what Singapore will look like in the next 50 years, IoT is both transformational and inspiring, but not without challenges. Smart technologies continue to be developed and deployed in our cities without a holistic cybersecurity strategy. As a result, Moore's law is playing out to hackers' advantage in that as data processing and storage costs fall we become less discerning about what data we store and send and how we store and send it.

For our future smart cities to prosper and bring in a new era of value creation, cybersecurity needs to be part of the IoT design and human resource development criteria. This new wave of innovation will continue to be disruptive, but it does not have to be destructive to smart cities with smart cyber solutions.

Challenges and Opportunities for Better Communication, Cooperation and Collaboration in International Cybersecurity in Asia

Challenges and Opportunities for Better Communication, Cooperation and Collaboration in International Cybersecurity in Asia

Yono Reksoprodjo, Lecturer and Researcher on Asymmetric Strategy Studies, Indonesia Defense University – (UNHAN)

Cyberspace presents both benefits and challenges to national security, economic prosperity and the social wellbeing of countries, affecting business as well as individuals. Given that today, states are increasingly becoming actors in cyberspace, including pursuing their national security interests, there is a need to collaborate and to enhance mutual trust. This should build transparency between states and develop measures to assist in preventing the risk of conflict caused by misperception and miscalculation between states in cyberspace.

Several international forums on cyber confidence building measures (CBMs) are being held regularly by many countries, including the ASEAN members, as well as other regional organisations. The purpose of such collaborative activities is to achieve a common understanding by providing transparency measures to enhance stability in cyberspace.

However to date, efforts to reach a common understanding on transparency as proposed by these cyber CBM forums seems far removed from states' real intention or willingness to share and exchange critical information. This might be the case due to the lack of understanding on the nature of the threats, in addition to what in fact is the best philosophy for correctly governing cyberspace. This is important since the national interest might be different in each country.

Challenges

Particularly with large cyber incidents, attacks have not always come from a single country or single source. Although a suspected state may attack directly, when it comes to cyber in order to remove traces of attack, utilising proxies is often a common tactical choice. Countries may use a proxy that may not necessarily know that they are being used, which means that there is a true possibility of an innocent country being involved.

In order to avoid this occurring, countries must have the capacity and capability to secure all of their cyber components and networks so that they cannot be used as an attack launching platform for other countries.[1] Nevertheless, no matter how good a country might be in building a cybersecurity ecosystem, in reality, it is almost impossible to maintain cybersecurity alone. Cyberspace is not built by one person, one company or one country but by many contributors and this will continue in the near future.

Therefore, each stakeholder has a role and responsibility to take good care of cyberspace. This is not a choice but a must. However, the question then becomes, how? Communication, the willingness to share information, and to be transparent will be key factors for successful cooperation and collaboration. All must work together to participate in providing stability in cyberspace and rise to the challenge of enhancing international collaboration in cybersecurity.

The ASEAN Regional Forum (ARF) CBM workshops have been designed as a platform for communication. The aim is to increase participants' knowledge and understanding of the role and the importance of confidence building and transparency measures in promoting stability in cyberspace. For example, there has been focus on a number of practical issues such as the importance of points of contact in each participating government to manage cyber crises and enhance common understanding of the types of measures that could be put in place to contribute to ensuring regional cyber stability. Further, it is expected that through good communication between points of contact

that mutual trust may be established as well as the exchange of important cybersecurity information.

In the near future, the ARF should also aim to establish a prevention mechanism like a threat risk reduction program. An effective incident response procedure for a cyber crisis is needed. There is a need for a mechanism that caters for damage rehabilitation and reconstruction to assist full recovery in the event of a total data loss.[2] This is why a concerted effort is needed by countries in the region to agree on terms and conditions that may then become a "Common Cybersecurity Code of Conduct". Communication, cooperation and collaboration are key in order to achieve cyber CBMs but trust will be the soul of successful communication, cooperation and collaboration in cybersecurity.

Opportunities

A willingness to understand different cultures will be important when beginning a dialogue on international cooperation and collaboration. The problem that often arises in international cooperation can lie in the use of different languages as well as different cultural values, beliefs, and ethics. Unfortunately, these are not easy to change. Although we can expect that individuals using cyberspace can read, write and are well updated on current world issues, not all may be necessarily aware or agree on what has become the "world's so called International Law". There are more people that only see international law as formed by western-centric international lawyers. Further, stereotyping and socio-typing are not always helpful because it degrades the trust factor needed for communication, cooperation and collaboration. Therefore, managing cultural value differences with a willingness to accept differences, to understand others, and to share and honour different values, beliefs and norms will be basic requirements.[3]

ASEAN members are those countries that represent many different ethnicities and languages. Indonesia alone has about 17,000 islands, 1,200 different

ethnicities and 750 languages. To deal with this, Indonesia has managed to find the right ways to handle cultural value differences and enable real harmonious co-existence. This provides an opportunity for all Indonesians to develop a high tolerance that then creates common trust. This can then provide comfort and mutual security. Within a sufficient period of time, based on mutual trust building, it should finally find the adhesive that holds a country like Indonesia living in harmony in a very diverse mix of cultures.[4] Following this example, knowing that people in ASEAN member countries are accustomed to living in diversity, we may learn to copy similar ways when building enhanced communication, cooperation and collaboration for cyberspace.

Some international activities like the Global Conference on Cyber Space 2015 (GCCS 2015), among others, have agreed on joint activities that encourage capacity building. The purpose of this activity is to build a global common perception on important issues in cybersecurity.[5] Unfortunately, the effort has not explicitly explained that the very basic perception needed is common cyber ethics that can be used as the basis of a moral compass in cyberspace. This will create cyber cultural values as the core to avert the abuse of cyberspace.

Many activities following GCCS 2015 as well as the activities of the ARF on cyber CBMs are important steps that can help achieve common understanding on how to come together to maintain a stable cyberspace. Such activities provide a platform to create mutual trust that is very much needed.

To conclude, normative ethical and moral behaviour is an important precursor to instil more order in cyberspace. Without these factors, it would be very difficult to govern cyberspace. Tolerance in understanding differences in cultural values will create opportunity for opening communication. And good communication would pave the way for fruitful cooperation and collaboration. We would then be able to work together to achieve the mutual trust needed to exhibit transparency in what is a “cyber build-up” and exchange of the critical information needed to create a stable cyberspace.

[1] The author understands “cyber components” to be “technologies and physical items like cloud, servers, HDs, FOs, etc”. Countries like Indonesia are encouraging discussion on cyber sovereignty. The author asserts that it is very important that a country that employs such technology or facility take full responsibility of the security of their systems.

[2] Yono Reksoprodjo, “Trends and Threats in Cybersecurity…so What?”, Asia Internet Symposium - Internet Society (ISOC) Jakarta Chapter, Jakarta, 7 September 2015.

[3] Yono Reksoprodjo, “Understanding Culture and Local Wisdom in Conducting Regional Cooperation”, Military Contribution to Regional Multilateral Cooperation, The 9th Pacific Army Chiefs Conference - The 39th Pacific Army Management Seminar, Bali, 15 September 2015.

[4] Wikipedia, “Daftar Pulau di Indonesia”; https://id.wikipedia.org/wiki/Daftar_pulau_di_Indonesia; See also: Wikipedia. “Indonesia”, https://en.wikipedia.org/wiki/Indonesia.

[5] Global Conference on Cyber Space 2015, https://www.gccs2015.com/, The Hague, 16-17 April 2015.

Global Implications of the United States – China Cyber Relationship

Global Implications of the United States – China Cyber Relationship

Jason Healey, Senior Research Scholar, Columbia University's School of International and Public Affairs

For those new to international cyber power and cyber conflict issues, a good rule of thumb is that China uses cyber capability because it is behind; Russia because it lost; and the United States because it won.

China, since the Unequal Treaties in the 1840s, has felt behind more developed European (and Japanese) powers. Nearly anything is justified to catch up, to redress that balance, and re-establish China as an equal power. Russia "lost" the Cold War, and so causes trouble in the territory it lost, engaging in conflicts (cyber and otherwise) in former Soviet republics and, to a lesser degree, against former Warsaw Pact adversaries.

Since the United States "won" the Cold War, as the remaining superpower it has felt competing needs. It wants both an open, safe and resilient Internet where borders are relatively unimportant, crime is relatively low, and information spreads mostly freely. It also wants the Internet as an area for supremacy for military and intelligence capabilities as part of a superpower's global responsibilities.

This article will examine some aspects of these Chinese and U.S. positions and some of the global implications.

Differing views

Chinese vulnerability in cyberspace, the feeling of being behind, is easy to understand.

Everywhere the Chinese look, they see Americans on the commanding heights of cyberspace. The protocols were designed by Americans and embody American values: "namely that it is open, nonhierarchical, self-organizing, and leaves essentially no opportunities for governance beyond protocol definition. Anywhere the Internet appears, it brings those values with it."[1] A significant portion of Internet traffic is still routed through the United States, and American companies dominate, from Apple and Microsoft, to Intel and Cisco, and Facebook and Twitter. U.S. Cyber Command and the National Security Agency seem to loom above all.

Especially when China's own technology companies were still rather small, the desire to use cyber espionage to bring American research and development to the Middle Kingdom to be commercialised must have seemed an easy one.[2] After all, the Chinese Communist Party has staked its legitimacy on continued economic success and becoming a great power again, no longer able to be bullied by the West.

Of course, China has always denied conducting commercial espionage and has now pledged with both the United States and United Kingdom not to ever do so.

China also uses cyber capabilities in other ways for domestic legitimacy, including blocking content deemed unhealthy for its citizens, taking down such content in servers overseas, and using denial of services attacks to shout down groups like Falun Gong that present a challenge. It has sometimes been useful to allow "patriotic hackers" to release nationalist steam by taking down offensive Japanese, Philippine, or American websites.[3]

In the United States, the debate on cyber power has been dominated by two major and sometimes overlapping sets of policies. The first set can be summed up as "Internet freedom" but covers a wide range of policies which reflects the U.S. "core commitments to fundamental freedoms, privacy, and the free flow of information."[4] This means an open and resilient Internet,

with few borders and relatively limited sovereignty. These policies are very heartfelt and are rooted in American hopes and values: the best of what Americans think of themselves and their nation's identity as the home of freedom and democracy.

The other American cyber policies are rooted not in American values, but in American fears and interests. These see the Internet as a domain to be hopefully dominated by American military and intelligence power, just as in the air, land, sea, and space. As the sole remaining superpower, such dominance is seen in national security circles as an actual American *responsibility*: no one else, in this view, has the power or willingness to address global scourges like terrorism or nuclear proliferation to unstable and despotic regimes. If it is not dominated by the United States, a democracy, it will be taken over by others far, far worse.

Flashpoints

There are of course areas of intense danger when two strong powers, with significant capabilities, have such differing viewpoints. With both nations feeling entitled to act with gusto and power, miscalculations and escalations are likely.

A chronic issue, which only occasionally boils over, is the control of cross-border content. The United States has a very strong position that speech should nearly always be allowed, even when it is unpleasant, wrong, or even dangerous. China, to put it lightly, disagrees, usually by blocking it with the Great Firewall and other mechanisms, but sometimes by conducting attacks against offensive material overseas, such as the 2015 attack on Github.[5] This issue will cause periodic political ructions, but little outright conflict.

In contrast, espionage by both nations has the chance to escalate into far more serious crises. President Xi Jinping of China has promised personally and publicly to President Obama that China does not conduct commercial

cyber espionage – never has, never will, as it were. With such a personal and public commitment, any significant perceived violations will immediately be a personal issue between the heads of state of the most powerful countries on earth.

In the other direction, U.S. espionage against China is almost certainly highly intrusive, if the Snowden revelations are any guide. It is not used for commercial, profit-making purposes as China's is, but this need not make it seem any less aggressive or escalatory. After all, even though the data in the U.S. Office of Personnel Management was admittedly a valid intelligence target, U.S. officials and politicians continue to call for retaliation.

A third flashpoint is related to U.S. and regional disagreements with China over territory, especially Taiwan and islands in the East and South China Seas. Another long-time rule of thumb to understand cyber conflict is that physical conflict begets cyber conflict. That is, if there are flare-ups between coast guards or even navies, then expect to see conflicts quickly follow in cyberspace.

This cyber escalation is most obvious in attacks by patriotic hackers but likely each side would increase all kinds of electronic surveillance of each other's military forces and potentially their intelligence preparations for strikes against supporting military bases and supply chains. At some point, this increased intelligence collection could become a flashpoint on its own, separate but related to the physical conflict which sparked it.

Implications

These flashpoints may have graver and more far-reaching implications than anticipated by traditional international relations and national security studies.

According to a classic piece of national security scholarship by Professor Robert Jervis of Columbia University, a security dilemma is "doubly dangerous"

if the offense is dominant over defense and it is hard to distinguish offense from defense.[6] Of course, this exactly describes the cyber domain.

But the situation in cyberspace is even more dangerous. In cyberspace, it is not just hard to distinguish offense from defense, but also to distinguish from espionage and intelligence preparation of the battlespace. There are very low barriers to entry for many nations and even non-states, and many adversaries freely use offense and espionage because of the difficulties of attribution.

Together, this might mean that cyber conflict might be the most escalatory kind of warfare that mankind has ever experienced. Flashpoints like those discussed above may have far more potential to spiral out of control than is realised in Beijing or Washington DC.

In addition, the stakes for the United States and China - and all nations depending on the Internet for increased innovation and productivity - are higher than expected. According to a recent study for the Atlantic Council, a drastic increase in cyber conflict and crime, such as from an escalating U.S.-China fight, could lead to perhaps *$90 trillion* less in global GDP through 2030. Even an increase of cyber sovereignty, of strong Internet borders such as China's, could lead to $30 trillion less in global GDP.

In these futures, security issues would take over all conversations at forums such as ASEAN, crowding out discussions of deeper and more productive issues such as trade or improved Internet resilience. This would affect everyone on the Internet, especially in the Asia-Pacific region, not just the United States and China.

There are areas of overlap where both nations can cooperate. The recent Obama-Xi agreement is a promising sign, especially if both sides hold to it over the next five years.[7] North Korea also, oddly, might help. After the country hacked Sony in late 2014, it appears the United States and China were both "riled" and had similar interest to rein in the country.[8]

With so much on the line, Asia-Pacific nations have much to lose if the United States and China cannot come to terms over cyberspace and much to gain if all nations, together, can compromise for a more peaceful and prosperous Internet.

---

1 Dan Geer, "A Time for Choosing", http://isen.com/blog/2011/01/dan-geer-a-time-for-choosing/, January 2011.

2 See the full book-length treatment of the full range of Chinese industrial espionage by William Hanna and James Mulvenon, Chinese Industrial Espionage: Technology Acquisition and Military Modernisation, 2013.

3 For example headlines, see http://yris.yira.org/essays/1447, http://www.theregister.co.uk/2012/04/27/philippine_china_hack_stand_off/ and http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html.

4 The White House, "US International Strategy for Cyberspace", https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 2011.

5 Bill Marczak (et al), "The Great Cannon", Citizen Lab, https://citizenlab.org/2015/04/chinas-great-cannon/, 10 April 2015.

6 Robert Jervis, "Cooperation Under the Security Dilemma," World Politics, http://www.jstor.org/stable/2009958?seq=1#page_scan_tab_contents, January 1978.

7 See, for example, Jason Healey, "Even if flawed, cybertheft deal a win for Obama", Passcode, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0925/Opinion-Even-if-flawed-cybertheft-deal-with-China-a-win-for-Obama, 25 September 2015.

8 Tom Risen, "China Likely Irked by North Korea's Sony Hack", US News, http://www.usnews.com/news/articles/2014/12/23/china-likely-irked-by-north-koreas-sony-hack, 23 December 2014.

Cyber Relations between the United States and China: A Chinese Perspective

Cyber Relations between the United States and China: A Chinese Perspective

Zhu Qichao, Director and Professor of the Center for National Security and Strategic Studies (CNSSS), National University of Defense Technology, China

The Internet has had a profound impact on China's governance and the life of individuals since it was introduced to the country in 1994. At the end of June 2015, China had the world's largest number of Internet users, nearly 668 million. Cybersecurity has become a serious challenge with the ceaseless emergence of Internet criminal acts, hacking attacks and leaks of private information. In addition, the use of the Internet by terrorists, religious extremists and extremist forces has helped to expand their influence globally.

Since around 2010, with the rapid development of China's comprehensive national power and the continuous expanding of its national interests in cyberspace, cybersecurity has become one of the most important issues with striking impact on the relationship between China and the United States. Topics such as cyber freedom, cyber sovereignty, hacking attacks, intellectual property espionage, a code of behaviour in cyberspace, among others, have always been mentioned and mutually-criticised by both think-tank scholars and government officials in both countries. During the period of 5 June 2013 (Edward Snowden's disclosure) to 19 May 2014 when the U.S. Department of Justice prosecuted the "so-called" five Chinese military members for cyber espionage, the fierce oral confrontation on cybersecurity issues between the two countries was thoroughly concerning to the international community. As a Brookings report notes, "There is perhaps no relationship as significant to the future of world politics as that between the U.S. and China…In the web of relationships that have built up between the U.S. and China, no issue has emerged of such importance, and generated such friction in so short a time span, as cybersecurity."

Cyber-related areas of friction between China and the U.S.

Given that there are outstanding differences on many issues (for example, political institutions, ideologies, development phases, historical and cultural traditions), it is inevitable for the two powers to hold different opinions on cybersecurity issues. This is especially the case for four specific issues: 1) Cyber freedom and cyber sovereignty; 2) Cyber hacking; 3) International Internet governance; and 4) Cyber arms control and an international code of action.

1) Cyber freedom and cyber sovereignty

From the perspective of the U.S. government, basic freedom in cyberspace should be protected, and the freedom of being interconnected and communicating information should not be restricted. Further, big powers such as China and Russia should not conduct any Internet content filtering or censorship. Whereas people from China and Russia may perceive that the U.S. always has a tendency to take advantage of so-called cyber diplomacy and cyber smart power to intervene or to even overturn adversary governments.

From the Chinese government's point of the view, there is no such thing as "absolute cyber freedom". Every country should comply with the United Nations Charter and those globally recognised basic principles of international relations – in other words, every country's sovereignty, territorial integrity, and political independence should be respected, as should diversity of histories, cultures and social institutions. In cyberspace, the principles of sovereignty and the principle of information flowing freely and securely should always be insisted upon, and every country in the world should prevent cyberspace from becoming a new tool for intervening in others' domestic affairs. In particular, cyber supremacy should not be exercised in the name of cyber freedom.

2) Cyber hacking

As a new type of international public nuisance, hackers' attacking has become more and more rampant, particularly since in terms of cyber it is easy to attack but hard to protect.

According to a 2013 CSIS report, "The Economic Impact of Cybercrime and Cyber Espionage", the United States lost almost 160 billion dollars annually on account of cybercrime - this accounts for around one per cent of its GDP. China's Internet security situation is not optimistic either. According to a CNCERT report released in 2013, theft of economic interests has become one of the major goals of hackers. And at the 4th Global Cyberspace Cooperation Summit held in November 2013, Cai Mingzhao, the Director of China's State Council Information Office, pointed out that more than 80 per cent of Chinese Internet users were once "cyber abused", thus amounting to losses of tens of billions of U.S. dollars annually.

Yet, some western countries, especially the U.S. government, think tanks and news media, always preferred to accuse hackers from China and Russia, among others, for cyber attacks and cyber espionage on their technological and commercial secrets. Following Snowden's disclosures, quite a lot of U.S. government officials, congressmen (and even the public) tend to believe that the so-called American national-security-oriented cyber spying is better than the so-called Chinese economic-interests-oriented cyber spying. Just one week after the U.S. declaration of the prosecution of Chinese military officers, the Chinese Internet News Research Center (under the State Council) enumerated the United States' global massive monitoring actions in the name of national security. Through Chinese official news media, we can see that the Chinese government is strongly vigilant of the U.S. motive of seeking supremacy in cyberspace with its superior position in information technology.

3) International Internet governance

Given every country's growing political, economic and social dependence on the Internet, China, Russia, and even some of the developed Western European countries have proposed that an international institution similar

to ITU should be established to replace ICANN and be responsible for the managing and allocating of Internet domain names and IP addresses.

Although the National Telecommunication and Information Administration of the U.S. Department of Commerce declared on 14 March 2014 that the U.S. government was willing to hand over the critical Internet domain names' administrative functions to an organisation of global stakeholders, this was with the pre-condition that as a first step in handing over these Internet governance rights, all the stakeholders should be called together to form a transfer program with "broad international support". Most Chinese are inclined to believe that such a declaration could be considered as a compromised response to global pressure caused by the Snowden revelations. However, it is still a long way to move all Internet governance rights out of U.S. government control. Technically speaking, the partial handing over of the administrative rights of the Internet domain names from ICANN is just a limited measure to keep the Internet open, and it should not be considered that the U.S. really wants to give up control of the Internet.

4) Cyber arms control and an international code of action

ICT has promoted the development of economic globalisation and proliferation of social informationisation[1]. It has made critical infrastructures such as financial and securities information systems, power grids, transportation management information systems, massive industrial control systems, among others, more dependent on cyberspace. And it has pushed military affairs to become more cyber-related.

In order to keep adapted to the development trends of the world's new military revolution, most of the military powers have released their own cybersecurity strategies; established cyber war forces; and the arms race in cyberspace has been warming up persistently. At the beginning of 2013, in order to seek absolute superiority and freedom of action in cyberspace, the U.S. Department of Defense approved the increase in size of its Cyber Command, from 900 to 4,900 personnel in 2015 and 6,000 by the end of 2016. Given that the U.S. has already established some powerful cyber war capabilities, the acts of

setting cyber war rules and legitimising cyber war would definitely intensify the doubts of developing countries like China and Russia.

In September 2011, four members of the Shanghai Cooperation Organization (SCO), including China, submitted a draft, *The International Code of Conduct for Information Security,* to the United Nations. The main objective of the draft was to determine the code of responsible conduct for states in the area of international information security in light of challenges and threats of a military-political, criminal and terrorist nature emerging in cyberspace. Unfortunately though, the proposal gained insufficient attention and response from the United States.

Dialogues and cooperation

In order to reduce friction and confrontations as well as to keep China-U.S. relations on the right track, the two powers have conducted multiple types of communication and cooperation for cybersecurity matters since 2009. These can be divided into two levels: non-governmental and governmental.

At non-governmental level, these have included Sino-American academic conferences, and Track 2 cybersecurity dialogues such as the CICIR-CSIS cyber dialogues in 2009, CNCERT- EWI in 2011, and Brookings in 2011/2012.

At governmental level, there has been dialogues between high-level government officials; cooperative mechanisms between functional departments; a governmental cyber working group under the Strategic and Security Dialogue framework (April 2013); and governmental experts have met to discuss cyber issues under the UN framework (June 2013). Moreover, both China and the U.S. have had effective cooperation through the Joint Law Enforcement Contact Group on several issues that include tackling cybercrimes, intellectual property law enforcement, and justice assistance. For example, in August 2011, Chinese and U.S. law enforcement authorities

jointly uncovered a Chinese porn website, Sunshine Entertainment Alliance – the biggest in the world.

Barriers affecting China-U.S. cooperation on cybersecurity issues

With the further extension of Chinese and American cyberspace interests, the need for cybersecurity cooperation between the two countries will become increasingly strong.

Positive cooperation will play a facilitative role in shaping the Sino-U.S. relationship. But it should not be denied that there still are some barriers affecting cybersecurity cooperation between the two powers. Apart from long-standing structural problems like economy, trade, and the Taiwan issue, among others, the following three issues need to be focused on with great care:

First, how would the U.S. handle the negative impacts of its rebalancing strategy? Since 2009, the U.S. has returned to Asia with a high profile and put forward the strategy of “Asia Pacific rebalancing”. The strategy mainly includes the TPP in the field of economy, the Air-Sea Battle Concept with China as the imaginary enemy, and strengthening the U.S.-Japan Alliance. These initiatives will inevitably increase the pressure on China’s national security concerns, and cast a lingering shadow on future cooperation on cybersecurity.

Second, would the U.S. be willing to accept China’s advocating for a “new type of relations between major powers”? Chinese leaders recently put forward the “new type of relations between major powers” - the connotation of which is “no conflict, no confrontation, mutual respect, cooperation, and win-win”. This new concept is based on the universally recognised norms of international relations, reflecting the responsibility and style of doing things in China as a big developing country. However, the U.S. believes in the principle

of power, and the basis of its national security strategy is to maintain global hegemony. As for whether the U.S. is willing to accept China as an equal partner rather than a potential strategic rival, the answer does not seem very optimistic. China and the U.S. may have different understandings of the position of "new relations between big powers", thus affecting the development of bilateral strategic mutual trust, and impacting the China-U.S. exchanges and cooperation that concern cybersecurity issues.

Third, would the U.S. positively self-restrain its build-up of cyber armaments? The U.S. has the world's most powerful military and the largest as well as most powerful cyber army. The high-profile military build-up of the U.S. Cyber Command since 2013 will be the reference point for the development of the world's cyber power. For China, the U.S., Russia and other major powers, the arms race in cyberspace will exacerbate strategic mutual suspicion between countries. Although U.S. scholars firstly proposed the concept of "strategic restraint", calling on Russia, as well as the U.S. and China to strategically restrain each other in the field of nuclear, space, and cyber, the sense of insecurity of other countries will be more intense if the most powerful country cannot restrain itself. Even some experts from the U.S. have begun to believe that it is the U.S. rather than China that is promoting the arms race in Asia. This indicates that if the U.S. does not adjust its Asia-Pacific security strategy and policy, what follows will be an endless arms race in the region, continuing to erode the fragile China-U.S. strategic mutual trust.

In addition, there are cognitive differences on cybersecurity issues. China and the U.S. have communicated with each other in various fields which are likely to be affected by cybersecurity. Yet, the differences in the extent of the development of social information, and the legal and political systems between these two countries means the dialogue, is not only at a shallow level, but it also causes cognitive dislocation. The first cognitive dislocation relates to the information technological edge. Since China is the biggest developing country with great potential, it has long considered that the U.S. occupies the world's unrivalled high-tech advantage, especially in the field of ICT. IT corporations like Cisco, Google, Oracle, and Microsoft have

often been regarded as in a monopoly position in terms of technology. In this aspect, China is considered inferior to the U.S., and it is even feared that China's cybersecurity is of no use, given the United States' powerful technological advantages. Nevertheless, while the U.S. may hold this position, because of the fast spread of technology and low threshold for innovation, some Chinese IT companies may even take up a comparative advantage. The U.S. is therefore afraid that cybersecurity is no longer as absolutely reliable as heretofore.

Implications for the future

Although China suspended the cyber working group activities since the U.S. Department of Justice indicted five Chinese military officers for hacking American corporations, the interdependence between the two countries is deepening. Fortunately, both governments have been wise enough to continue talking about cybersecurity issues recently during the new round of strategic and economic dialogue in 2015.

In general, China-U.S. cybersecurity cooperation faces not only constraints but also opportunities. Looking forward, if the U.S. can really treat China as an equal partner and accept the construction of a new pattern of relations between great powers as put forward by China, it will help consolidate the foundation of mutual trust through pragmatic cooperation, thus also breaking barriers that affect cybersecurity cooperation. It should be pointed out that the China-U.S. competition in cybersecurity issues is based on their competition in terms of strength and their cooperation should also be based on their strength of cooperation. If there are significant differences between two great powers in strategic decision-making capabilities, information technology capabilities, and cyber defence strength when dealing with cybersecurity challenges, the true equality of bilateral cooperation will be difficult to achieve.

In addition, apart from tackling cyber relations with the U.S., China has been active in bilateral and multilateral dialogues in relation to cybersecurity

with the UK, South Korea, ASEAN, the European Union and Africa Union, among others. It is trying to carry on even more substantial cooperation with all relevant parties. Furthermore, China and ASEAN co-sponsored the Cyberspace Forum last September aiming to build a shared cyberspace community. This is a very important part in the framework of China's newly delivered "The Belt and Road Initiative", as well as the Internet Plus Initiative.

In the author's opinion, China will keep to its policy of cyber cooperation in the future. As President Xi Jinping stated, following the principles of mutual respect and mutual trust, China is ready to work with all other countries to deepen international cooperation, respect sovereignty on the Internet, uphold cybersecurity, and jointly build a cyberspace of peace, security, openness and cooperation, as well as an international Internet governance system of multilateralism, democracy and transparency. The Belt and Road Initiative as well as the Internet Plus Initiative will make China the backbone of the global Internet industry, both in terms of user numbers and the market values of the Internet companies. Robust cyber relations between China and the U.S. will contribute to the world as an important security stabiliser and vigorous innovation enabler.

---

[1] The author understands the term social informationisation to mean "the process to shape or upgrade the style of social life and the pattern of public management with the development and application of ICT and information systems".

Lethal Autonomous and Cyber Weapons – Do They Challenge International Humanitarian Law?

Lethal Autonomous and Cyber Weapons – Do They Challenge International Humanitarian Law?

William H Boothby, Air Commodore (Retired)

To reach a sensible answer to this complex question, it is necessary to establish what exactly the notions of lethal autonomous and cyber weapons refer to, to consider how international law addresses new kinds of weaponry, and to then assess how the relevant legal rules apply. These three elements will be discussed in sequence.

What are lethal autonomous and cyber weapons?

Recent years have seen numerous attack missions undertaken by Predator and Reaper remotely piloted aircraft (RPA).[1] Such 'remote control' technology is also to be found in the land, maritime and undersea environments. Increasingly, automation and even levels of autonomy are being introduced into unmanned weapons systems. While there are numerous examples, the U.S. Aegis Ballistic Missile Defence System which detects and responds to inbound threats such as rockets, the U.S. Mark 15 Phalanx system that automatically engages anti-ship threats, and the Israeli Iron Dome system that counters the rocket threat (from Gaza for instance) demonstrate this developing trend.[2]

So what do 'automation' and 'autonomy' mean in the current context? Of note, applicable international law makes no mention of these terms. UK military doctrine describes automation in terms of systems that respond to sensor inputs and act according to pre-defined rules. Essentially, it is the pre-set nature of those rules that means that the action that the weapon system will take is somewhat predictable.

Autonomous systems, on the other hand, understand higher-level direction, are aware of the environment in which they are operating and can make

higher-level decisions. Such a system can independently identify and attack targets without being programmed to attack a specific target.[3] For the purposes of the focus of this article on international humanitarian law, it is an essential element in autonomy that the machine is being given the task of making its own decisions over attack with no human participation when that specific decision is made. Nevertheless, there is still some dispute among observers over when true autonomy will in fact be realised.

In relation to the cyber sphere, the experts who produced the Tallinn Manual felt that notions of 'attack' and 'weapons', well recognised in the law of armed conflict, also make sense in the cyber domain.[4] They concluded that it is the death, injury, damage or destruction that a cyber operation causes that qualify it as a cyber attack. So cyber capabilities that are used, designed or intended for use for such purposes become cyber weapons to which the law of weaponry can be applied.[5] It should be noted that Russia and China interpret cyber activities by reference to notions of the information space and that those states would be unlikely, at the time of writing, to endorse the Tallinn Manual analysis in full.[6]

International law and new weapon technologies

A fundamental principle that binds all states asserts that the right to choose weapons, weapon systems and ways of conducting conflict is not unlimited. International law prescribes the applicable limits.

The 174 States party to Additional Protocol I of 1977 (API) are required in the study, development, acquisition or adoption of a new weapon, means or method of warfare to determine whether its employment would in some or all circumstances conflict with the international law applying to the State.[7] Existing law is the yardstick against which new technologies must be judged.[8] Therefore, it is important to determine what existing principles and rules determine the lawfulness of new weapons.

All states must apply the following two customary principles: 1) The State is prohibited to use a weapon or way of conducting conflict that is of a nature to cause superfluous injury or unnecessary suffering;[9] and 2) The State is prohibited to use a weapon or way of conducting conflict that is indiscriminate by nature.[10]

States party to API are also prohibited to use weapons that are intended or may be expected to cause widespread, long-term and severe damage to the natural environment - this represents the third rule against which a new weapon should be judged.[11] However, this rule has yet to achieve customary status.

Furthermore, there are numerous rules in the law of armed conflict that prohibit, or respectively restrict the circumstances of lawful use, of particular kinds of weapon or weapon technology.[12] There are, however, no law of armed conflict rules that are explicitly stated to apply to cyber weapons or to lethal autonomous weapons technology.

As to the three remaining rules summarised above, the autonomous nature of the functioning of a weapon system does not have any relevance to the degree or nature of the injury or suffering that will be caused to any individual that may be targeted. Rather, it is the projectile, the missile, the bomb or other weapon that the system fires that will determine the nature of the injury or suffering. Similarly, the injury or suffering occasioned by a cyber weapon will not be dependent on its cyber character but, rather, on the nature and manner of engagement of the target at which it is directed. For essentially similar reasons, the environmental protection rule is unlikely to be relevant to the autonomous or cyber character of the weapon.

The indiscriminate weapons principle prohibits weapons that cannot be directed at a specific lawful target or the effects of which cannot be appropriately limited and which accordingly strike lawful targets and civilians and civilian objects without distinction. It is likely that any autonomous and

most cyber weapons will have been designed to seek out, identify and engage the intended target as accurately and reliably as possible, so in most cases it may not be hard to establish that the rule does not breach the indiscriminate weapons principle.[13]

Issues concerning autonomous and certain cyber weapons

Autonomous weapons, including cyber weapons that operate autonomously, raise additional legal concerns which should be carefully considered before any decision is made to procure and/or field such a weapon. This is because autonomous weapons in general, and certain cyber weapons, exclude the human operator from the decision whether to prosecute a particular attack.

Contrast an RPA such as Predator or Reaper, the operator of which is fed data from the RPA and from other sources. That operator makes the attack decision in a similar but not identical way to the pilot of a manned aircraft; is often referred to as the 'man in the loop'; and has the responsibility, and practical possibility, of applying the targeting rules in articles 48 to 67 of API and in customary law.

'Man on the loop' weapon systems, on the other hand, have the capacity for the weapon system itself to decide which target is to be attacked, but task a human being to monitor those decisions, to intervene if necessary and to stop autonomously-made attack decisions that for whatever reasons, including targeting law reasons, would be unacceptable. That man or woman 'on the loop', if not excessively tasked and if the system is operating correctly, is able to ensure that targeting law rules are complied with.

However, with autonomous and certain cyber weapon systems, the decision as to whom or what to attack is left to a weapon system that is not monitored by a 'man on the loop'.

The critical issue is therefore whether the system can be used in accordance with targeting law. The following questions reflect some of the decisions prescribed by the law of targeting relevant to such a weapon system:

a) Will the weapon system limit attacks to lawful targets?;[14]
b) Can it distinguish combatants (in other words, members of the armed forces who are not medical and religious personnel or members of a *levee en masse*) from civilians, medical and religious personnel or persons *hors de combat?;*
c) Can it determine the civilian damage and losses to be expected from an attack and compare these with the military advantage it is anticipated to yield?;[15]
d) Can it determine whether the circumstances permit the giving of a warning and, if so, can it give one?;[16]
e) Can it decide whether an alternative weapon or way of attacking would minimise civilian dangers?;[17] and
f) Will it know if another target would give a similar military advantage but involve less danger for civilians?[18]

Consequently, the challenge for autonomous, highly automated and some cyber systems becomes particularly acute with the evaluative targeting law obligations. Technology to enable a machine to determine what civilian damage and injury are to be expected, what military advantage is anticipated and to assess whether the former is excessive in relation to the latter is not, so far as the author is aware, currently available. Likewise, and again by way of example, there would seem to be no currently available system logic to enable a weapon to distinguish between a combatant who no longer has means of defence and one who, though wounded or sick, still does.[19]

Of particular note, advances in computer hacking techniques, combined with the introduction of weapon systems that increasingly rely on computer control or support, and indeed the growing reliance of targeting processes on computerised arrangements all suggest that hacking into and manipulation of the enemy's military computer infrastructure will increase in the future. That

in turn suggests the need to ensure the robustness of those very systems against intrusion and interference.

There is no war crime for failing to take the precautions in attack required by article 57 of API, but a weapon system that does not permit such precautions to be taken in the intended circumstances of use is a weapon system that should be rejected on weapon review. That at least would seem to be the legal position in relation to autonomous kinetic or cyber systems that seek out targets for offensive attack. Taking precautions in advance of a cyber attack may imply cyber mapping operations. That activity may, however, disclose and thus potentially frustrate the planned attack. Nevertheless, while the article 57(2)(i) and (ii) obligations are limited to feasible precautions, some precautions must be taken and attacking 'blind' will be unacceptable.

In relation to autonomy, contrast what might be described as 'point defence or platform defence weapons' such as the Israeli Iron Dome and the Naval Phalanx system. If the precautions required by targeting law can be adequately taken in advance of the deployment of such 'point or platform defence' systems, this would seem to enable such a system to be used lawfully. Much will of course inevitably depend on the design and performance of any particular weapon system. So it will be critical to establish that the software of the weapon system does in fact ensure that only lawful targets are engaged. Testing and empirical performance will inform that determination.

In the case of autonomous offensive attack, if a person must remain sufficiently on the loop to enable autonomy to be used lawfully, perhaps one might just as well use an RPA.

More recently, Human Rights Watch called for a ban of a broad selection of autonomous and, arguably, of some automated weapons.[20] A ban would, however, seem to be premature. Consider the possibility for instance that in the future more mature autonomous systems might actually involve more reliable compliance with the distinction and discrimination principles. The preferred approach, in the author's view, is for all states to legally review

the study, development, acquisition or adoption of any weapon technologies discussed in this article. Proper application of the relevant rules should result in the rejection at weapon review of currently available offensive attack autonomous weapons for the reasons discussed in the article.

To conclude, autonomy in the future is likely to feature in both kinetic and cyber weapon systems. It seems unlikely that new treaty law will address such technologies *ad hoc.* The existing rules prescribed by the law of armed conflict must be applied and the obligation legally to review new weapons applies to all states. However, there are differences of approach over cyber as between the West and Russia and China, and China seems likely to grow even further in importance in cyber matters in the next few years. The technology is developing rapidly, and cyber warfare seems likely to include intrusion and manipulation, which implies the need for further robustness in weapon control and targeting support systems.

---

[1] For Reaper Remotely Piloted Aircraft: See the announcement on 13 May 2011 of the formation of 13 Squadron to control the use of Reaper remotely piloted aircraft from RAF Waddington, available at https://www.gov.uk/government/news/raf-announces-new-reaper-squadron. Consider also Mapping US drone and Islamic militant attacks in Pakistan, BBC News, 22 July 2010, available at: http://www.bbc.co.uk/news/world-south-asia-10648909 and the increased US reliance on unmanned capabilities such as that afforded by the Predator UCAV; Predator Drones and Unmanned Aerial Vehicles, New York Times, 13 March 2013 See also S Casey-Maslen, Pandora's Box? Drone Strikes under jus ad bellum, jus in bello and international human rights law, 94 IRRC 597 (2012) at page 598-600.

[2] Consider for example the Phalanx system in service with the Royal Navy and described at http://www.royalnavy.mod.uk/The-Fleet/Ships/Weapons-Systems/Phalanx; the United States Navy MK 15 - Phalanx Close-In Weapons System, described at http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2; and the Russian Arena-E Active Protection System; the Mutual Active Protection System; the Diehl BGT Mutual Active Protection System described at www.defense-update.com/20110112_maps.html.

[3] See the UK Ministry of Defence Joint Doctrine Note 2/11, The UK Approach to Unmanned Aircraft Systems dated 30 March 2011 (JDN 2/11) issued by the UK Development Concepts and Doctrine Centre (DCDC) at paragraph 205.

[4] Tallinn Manual on the International Law applicable to Cyber Warfare (2013) prepared by the International Group of Experts at the invitation of the NATO Cyber Defence Centre of Excellence, Tallinn, Estonia (Tallinn Manual). The Tallinn Manual is not a source of law as such, as to which consider the Statute of the International Court of Justice, article 38. The black letter rules in the Manual reflect the collective view of the International Group of Experts as to what the law is.

[5] Note Tallinn Manual, Commentary accompanying Rule 41, paragraph 2. As to the status in law of the Tallinn Manual, see Wolff Heintschel von Heinegg, The Tallinn Manual and International Cyber Security Law, 15 Yearbook of International Humanitarian Law 3 (2012).

[6] However, the most recent report of the UN Group of Governmental Experts recognises that a number of States are developing Information and Telecommunications (ICT) capabilities for military purposes, that the use of ICTs in future conflicts between States is becoming more likely, and that there is a real and serious risk of harmful ICT attacks against critical infrastructure. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 dated 22 July 2015 presented to the 70th Session of the UN General Assembly, paras 4 and 5.

[7] See www.icrc.org, last accessed 3 September 2015.

[8] API, articles 35(1) and 36.

[9] API, article 35(2). This is a customary principle that therefore binds all states.

[10] API, article 51(4)(b) and (c). This is a customary principle that therefore binds all states.

[11] API, articles 35(3) and 55. This rule has yet to achieve customary status.

[12] For a discussion of the rules of weapons law, see, for example W H Boothby, Weapons and the Law of Armed Conflict (2009) (new edition forthcoming in 2016).

[13] Consider the Stuxnet attack on the computer system that regulated the operation of Iranian centrifuges at a nuclear processing plant. The cyber malware employed in the operation infected numerous other computer systems but reportedly in a non-damaging way. Such passive infection with no adverse consequences for the operation of the affected computer or for its users would not as such render the cyber weapon indiscriminate.

[14] Consider the principle of distinction, as reflected in API, articles 48, 51, 52 and 57(1).

[15] API, article 51(5)(b).

[16] API, article 57(2)(c).

[17] API, article 57(2)(a)(ii).

[18] API, article 57(3).

[19] See API, article 41 and note that a person only comes within article 41(2)(c) if he is rendered unconscious or otherwise incapacitated by wounds or sickness and is therefore incapable of defending himself and if he refrains from any hostile act and makes no attempt to escape.

[20] Human Rights Watch, Losing Humanity: The Case against Killer Robots, http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf, November 2012.

Technology, Threats and Trust in an Interconnected World

Technology, Threats and Trust in an Interconnected World

Robert J. Butler, Senior Advisor to The Chertoff Group

The Internet of Things (IoT) is the defining technological trend of our world today, breaking down the traditional barrier between information and operational technology by connecting devices in addition to and independently of their users. The IoT is redefining opportunities for the world as well as creating an increasingly interconnected global society. This article explores the impact and challenges of the interrelated ideas of technology, threats, and trust in an increasingly interconnected world.[1]

Technology

The IoT describes the ability to connect any device with an on and off switch (wired or wireless) to the Internet.[2] These devices could include a thermostat, car, or a pill swallowed so the doctor can monitor the health of one's digestive tract. These connected devices use the Internet to transmit, compile, and analyse data. Scale, capability and reach are its defining characteristics.

This therefore raises certain questions like what is driving the momentum we are seeing today? And why now? According to Goldman Sachs Global Investment and other research sources, there are around a half dozen trends that are the key enablers.[3] These include the following: 1) Cheap bandwidth; 2) Cheap processing; 3) Smartphones[4]; 4) Ubiquitous wireless coverage; 5) Big Data; and 6) Increasingly available strong cryptography.

In short, the cost of connectivity has declined at the same time that new ways to analyse mountains of data have developed and are still developing. As a result, governments and companies alike are focused on the IoT as a driver for technological edge and new capabilities. For example, since the beginning of 2014, AT&T in the U.S. has introduced a Connected Car service

in partnership with a number of automobile manufacturers, including Audi, GM, Tesla and Volvo, which offer high-speed 3G or 4G connections for a monthly subscription fee of USD$10. Thirty of GM's 2015 vehicle models now have LTE support, enabling vehicles to act as a Wi-Fi hotspot with connectivity for up to seven devices, as well as access to OnStar for remote vehicle access, diagnostics and emergency service.[5] Additionally, businesses are also embracing the IoT to improve productivity and save costs, especially in the areas of labour and energy. For example, in Singapore, the employment of software-defined modular data centers is resulting in significant operational cost savings.

The Internet is expanding in new and exciting ways. Expanding the telecom, cable, and satellite "pipelines" that carry traffic through broader Wi-Fi networks is a critical part. But providing devices with the sensor, memory chips and software necessary to communicate with the network is also key. Moreover, riding on this super-charged network of expanded pathways will be a wave of data. Big data is characterised by volume, velocity and variety. Ninety per cent of the data in the world today has been created in the past two years and that data is now forecasted to double every two years through the year 2020.[6]

However, combined with global connectivity and big data, the IoT creates concerns about threat vulnerability, overall security, and privacy.

Threat

According to a report published by the U.S. Federal Trade Commission (FTC) in January 2015, IoT devices can present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorised access and misuse of personal information (for example, exploitation of personal identity data on a smart TV;) (2) facilitating attacks on other systems (cascading DDOS attacks through interconnected POS and HVAC systems); and (3) creating safety risks, such as automated cars "gone wild".[7] Although

these risks exist with traditional computers and computer networks, they are heightened with the convergence of information and operational technology taking place in the IoT.

In addition to security risks, the FTC report identifies privacy risks flowing from the IoT. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, and health information. Other risks arise from the collection of personal information, habits, locations, and physical conditions over time that may subsequently allow an entity that has not directly collected sensitive information to then infer it.

These are all technology-driven risks that could be exploited by threat actors. It is clear that nations and surrogates are already using the advances in information technology to disrupt, degrade and/or destroy the economic opportunities and prosperity others have created and will continue to create through the IoT. The world of interconnected information technology has truly changed the global economy and national security engagement. Cyberspace is now the domain of cooperation, competition, and conflict. And in an interconnected world with unequal resource distribution, cooperation and competition are key - when they fail, conflict emerges.

We are also living in a world where national, provincial and local governments are critically dependent upon common, secure critical infrastructure services – services that need to be “on” 100 per cent of the time. Moreover, we are moving to a world where citizens in the Asia Pacific region and around the globe can only be safe and secure if communities and nations move with knowledge and speed to continually mitigate global risk. This can be achieved by having resilient structures at all levels that can shift resources automatically to disrupted or destroyed areas. And in order to do this, we need shared intelligence and partnerships. We must also learn to effectively use the IoT and big data for innovation and risk mitigation by enhancing trust.

Trust

In response to mounting concerns over data privacy, data security, and the rise of online surveillance, many governments have been seeking to pass new data protection rules. Several governments, including Germany, Indonesia, Russia and Brazil, are working toward enacting “data localisation” laws that would require the storage, analysis and processing of citizen and corporate data to occur only within their borders.[8] Proponents of these rules assert that by keeping data storage and processing close to home, they can provide their citizens and corporations with better defences against foreign surveillance as well as protection from the ambiguities of international data privacy rules.

Yet many of these proposals are likely to impose economic harm, and sow seeds of distrust within and across governments and industry. For example, several of the proposals under consideration would force companies to build servers in locations where the high price of local energy and the lack of trained engineers could translate into higher costs and reduced efficiencies, in effect defeating the IoT advances previously outlined. Furthermore, requiring that data reside in a server based in a host nation state instead of another nation will do little to prevent spies from accessing that data if they are determined and capable.

It is critical that both policymakers and technology providers, who must also take an active role in data protection, work together to develop solutions that keep the flow of information and online services available to all who rely on them. They must develop principles, norms and standards that can create a framework for coordinated multilateral action between states and across public and private sectors. They must also build partnerships of trust to act on these norms and principles. Computer Emergency Response Teams, Information Sharing and Analysis Centers, and new INTERPOL activities, such as the Global Center for Innovation (IGCI), represent some of the best models for building trust across private and public sectors within the Asia Pacific region and the globe.

Conclusion

As technology, especially the IoT, continues to advance, new threats emerge. Those threats come from nation states, terrorists and transnational groups, other politically motivated groups and cyber criminals.

In response to these threats, the identification of short and long term goals to improve privacy and security is imperative. Incorporation of privacy and security policies as well as principles will aid corporations and smart cities alike in an effort to combat growing digital threats. Key to addressing these threats is trust, and trust begins with partners committing to common goals and objectives.

New partnerships should be built and existing partnerships bolstered. In sum, we need to decide how to embrace technology, and deal with threats, and using this knowledge, shape an environment for trust and partnership in the Asia Pacific region.

---

1 This article builds and expands upon the technology/threat/trust interrelationship presented at The Chertoff Group security series in Houston/TX, 6 March 2015.

2 Jacob Morgan, "A Simple Explanation of 'The Internet of Things'", Forbes, 13 May 2014.

3 The Goldman Sachs Group Inc., "Internet of Things – Volume 2 Software and the IoT: Platforms, data, and analytics", http://www.wisburg.com/wp-content/uploads/2014/09/%E9%AB%98%E7%9B%9B-Software-and-the-IoT%EF%BC%9A%EF%BC%9APlatforms-data-and-analytics-The-role-of-software-acros.pdf, 2014.

4 See http://www.io.com//

5 Lynn Walford, "GM announces pricing for its 4G LTE service, to debut in 2015 Chevrolet Malibu", Tech Hive, http://www.techhive.com/article/2154720/gm-announces-pricing-for-its-4g-lte-service-to-debut-in-2015-chevrolet-malibu.html, 13 May 2014.

6 Marc Benioff, "Shaping a New Constitution for the Digital Age", The Huffington Post, http://www.huffingtonpost.com/marc-benioff/shaping-a-new-constitution-for-the-digital-age_b_7222014.html, 6 May 2015.

7 Federal Trade Commission, "Internet of Things: Privacy & Security in a Connected World", Staff Report, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, January 2015.

8 Bob Butler, Irving Lachow, and Jonah Force Hill, "Cloud computing under siege", FCW, http://fcw.com/articles/2014/09/12/cloud-under-siege.aspx, 12 September 2014.

The European Union's Approach to Cybersecurity and Defence

The European Union's Approach to Cybersecurity and Defence[1]

Wolfgang Röhrig, Programme Manager Cyber Defence at the European Defence Agency

For modern societies, information and communication technologies (ICT) are a critical enabler for economic growth and societies now rely on cyberspace in many different ways and on many different levels. Digitalisation has brought enormous benefits, but also new risks, which materialise through steadily increasing malicious activities in cyberspace. The impact of such malicious cyber activities can range nowadays from simple inconvenience to reputational damage, loss or compromise of information or even physical damage and loss of life.

While the history and track record of civil cybersecurity efforts in the European Union (EU) dates back as far as the early 2000s (when for instance, the European Network and Information Security Agency (ENISA) was established in 2004), the history of the military dimension of cybersecurity, in other words cyber defence, is relatively young. The topic first entered the agenda of an EU entity in 2011 when the EU Member States that participate in the European Defence Agency (EDA) decided with the revision of the Capability Development Plan (CDP) to place Cyber Defence Capability Development on the agenda of this agency.[2] Since then, the EDA has both conveyed several capability development and Research & Technology (R&T) projects alongside the tasking given by the 2011 CDP, while also actively supporting the development of the strategic and political framework, in which cyber defence in the context of the EU Common Security and Defence Policy (CSDP) is embedded.

The EU Cyber Security Strategy and its impact on the defence sector

The EU published its "Cyber Security Strategy – An Open, Safe and Secure Cyberspace" in February 2013.[3] The 2013 Cyber Security Strategy takes, like other national cybersecurity strategies, a comprehensive, holistic and whole-of-union approach. It addresses, within the remit of responsibilities that EU Member States have delegated or given to the EU, the civil aspects of cybersecurity as well as cyber defence for CSDP. Then, in December 2013, at the European Council on defence matters, the heads of state and government of the EU Member States recognised cyber defence as a priority for capability development.[4] The Council also tasked the European External Action Service (EEAS), of which the EU Military Staff (EUMS) is an integral part, to develop a Cyber Defence Policy Framework.

Cyberspace is now widely recognised by the military in EU Member States as a fifth operational domain besides land, sea, air and space. In addition, the success of conventional military operations in these other domains is enabled by, and dependent on the assured availability of, and access to, cyberspace.

For instance, current and evolving cyber threats must be seen in the context of several military implications that include:

- Conventional military activity relies on ensured access to cyberspace;
- The military is increasingly dependent on civil (critical) infrastructures – both at home base and in the operational theatre;
- As the military become increasingly interconnected using Internet technologies, Internet vulnerabilities are closer to individual soldiers and their weapon systems;
- The military can no longer afford the cost of not adopting commercial Internet technologies for their expanding networks. Thus military capabilities are susceptible to the same threats and vulnerabilities as the civil sector.

Moreover, the cyber activities of different war-fighting actors, both during a crisis as well as the different stages of a military crisis management operation, can serve the following purposes:

- Intelligence gathering to enhance own situational awareness
- Sabotage to take systems or assets of adversaries out of function
- Fundraising through cybercrime
- Positioning in adversary networks from which they can then conduct actions later in the course of conflict
- Subversion as well as influence activities

The defence part of the EU Cyber Security Strategy defines four major objectives: 1) Building of cyber defence capabilities with EU Member States; 2) Building the EU Cyber Defence Policy Framework; 3) Promoting civil-military dialogue; and 4) Dialogue with international partners like NATO and other major stakeholders.

The defence related strategic priorities of the EU Cyber Security Strategy were thus augmented by the EU Cyber Defence Policy Framework in November 2014. This framework further details the defence related tasking into 43 different lines of activity and allocates clear responsibilities for those lines of activities.[5] The second report on the progress of implementation of this policy framework was presented in November 2015 to the Policy and Security Committee of the Council.

Cyber defence for CSDP

In order to understand the EU's approach to cyber defence for CSDP, it is important to consider the following aspects. First, the EU is solely engaged in cyber self-protection and assured access to cyberspace to enable conventional military activity. Offensive cyber capabilities have not been developed, or deployed, under the EU banner. Second, the EU does not have standing military forces or EU-owned military equipment for EU operations. When

the EU launches a military operation, the EU is fully dependent on force contributions from EU Member States or other force contributors.

Based on these basic principles, the EU Member States are also the key to force generation with respect to cyber defence capabilities for an EU-led operation. It is in the interest of the EU to encourage and support them in their efforts to develop and maintain cyber inventories. In light of this, a 2013 EDA Cyber Defence Landscaping Study provided a detailed picture of capabilities, capacities and concepts already in place in EU Member States and EU institutions, entities and bodies that could be drawn upon to make CSDP operations more "cyber resilient".[6] The study revealed that the level of cyber defence capability varies strongly between Member States. In order to be effective, the EU and its Member States must develop, maintain and deploy a robust inventory of in-depth (layered) cyber defence capability for the military, as part of their national cyber defence strategies and capabilities. The EU and its Member States have to be prepared to proactively anticipate, prevent and defend against cyber attacks, and dissuade potential hostile actors through rendering cyber attacks ineffective by limiting their impact. The ability to attribute the origin of potentially hostile cyber activity could further enhance cyber defence. Furthermore, dissuasion of cyber attacks can be strengthened by improving resiliency as a matter of priority and by ensuring that timely and effective cyber defences deny meaningful gains to potential adversaries.

Like in any other military capability domain, success in cyber defence depends on a balanced combination of competent personnel, connected through well-developed processes and procedures, and applying state-of-the-art technology.[7]

People

The public perception is often that cyber protection is primarily a technological rather than a human issue. Today, all personnel at all levels require an increasingly sophisticated understanding of cyberspace and how to operate

effectively in cyberspace. Competencies and skills have to be developed and maintained. Cyber defence is not limited to cyber defence specialists. In addition, users of ICT, in other words, almost everybody in the military, has a role to play in cyber defence. They must have up to date knowledge and awareness of the contemporary threats and how to react in the event of incidents. This awareness should be frequently updated and tested as appropriate. Moreover, decision-makers must understand the cyber options and the impact of cyber operations when making decisions.

By way of example, cyber modules are now included in both general courses and specific cyber defence courses at the European Security and Defence College. In addition, more specific courses are currently under development in a common effort, under the lead of France and Portugal, in the Military Training Working Group of the EU Military Committee (EUMC) to grow the competencies and skills of the different stakeholder groups in the EU and its Member States.

Cyber awareness seminars for staff and deployed personnel have also been developed by the EDA. Furthermore, the EDA has developed a framework of necessary competencies and skills for the different stakeholder groups with respect to cyber defence. In addition to the value of the framework for the development of new course curricula, this can also serve to augment different job descriptions as necessary with required cybersecurity/defence competencies.

Processes

For the planning and execution of military operations, Standard Operating Procedures for cyber defence information sharing, situation awareness, incident response, business continuity, and disaster recovery have to be in place as well as frequently exercised and tested. In terms of practical support to military operations, an initial set of operational concepts and references has been developed over the last few years. For instance, the “EU Concept for Cyber Defence for EU-led Military Operations” was agreed in December 2012 – this is the EU military guidance for operational and

force commanders to create and maintain cyber situational awareness.[8] The Concept outlines the need to adopt a risk-based threat assessment methodology and to create coordinating structures to ensure that national cyber defence capabilities work coherently to protect the Force. EU Member States augmented the concept in March 2013 with the "EU Cyber Defence Capability Requirements Statement".[9]

In addition, on account of the EU's participation from early 2013 in the cyber defence focus area of the US-led Multinational Capability Development Campaign (MCDC), additional supporting documents for cyber defence planning for CSDP operations are available since late 2014. The EUMS and EDA also engage in the cyber defence work strand of the MCDC 2015-2016 campaign, which aims to develop in a multinational environment with 16 partners a cyber defence concept for the execution phase of multinational military operations.

State-of-the-art-technology

It is not possible today to provide a 100 per cent guarantee that clever attackers will not be able to penetrate networks and assets or that these attacks will not spill over into other networks or assets. Therefore, the disruption of an attack or at least the containment of the impact is, with respect to business continuity, the most important priority in order to keep the initiative and freedom of movement so as to achieve the given mission and tasks, including in cyberspace. In order to support the military decision-making process with respect to new cyber challenges, commanders must have the right technical toolbox to achieve and maintain cyber situation awareness as well as the technology to react to and mitigate the impact of successful attacks as well as to proactively protect own networks and military assets.

To strengthen such protection and response capabilities for CSDP operations, in 2013 the EDA developed (along the NATO Architecture Framework (NAF.V.3)), a cyber defence focused enterprise architecture for CSDP operations, which determines the general functional and technical requirements. The EDA also established a Research and Technology Project

to better detect Advanced Persistent Threat Malware. The project was due to deliver its results at the end of 2015. In addition, the EDA scoping for Ad Hoc Projects under the Pooling & Sharing Agenda for Multinational Cooperation on Cyber Defence Training, Exercise & Testing Ranges ("Cyber Ranges") as well as for Cyber Situation Awareness Packages for Headquarters (CySAP) has started. For both, the project implementation is envisaged to start in 2016. More subjects for technology development have been identified in a strategic cyber defence research agenda, which identified 99 military relevant research topics in order to close existing technology gaps where the markets do not currently offer satisfying solutions.

Cyber defence cooperation between EU Member States

In the rapidly evolving cyber threat landscape, it may not be possible to establish, maintain and use a cyber defence capability effectively without cooperation. Countries, especially small ones, find it often difficult, or unaffordable, to continue developing cyber capability on a national basis. For such countries, both cooperation and sharing development costs, is essential, rather than desirable, when developing and maintaining capabilities.

Cyber defence is certainly an issue with much sensitivity. Cooperation in cyber defence is about trust amongst partners with shared interests and requirements. And if there is trust, common interest, and willingness to cooperate, many options for synergies become real opportunities. This approach is also used in many other capability domains in defence. Whether to cooperate, with whom to cooperate, and the extent of that cooperation are sovereign decisions. However, sovereignty itself is not the decisive factor - trust and shared interest are more powerful drivers when deciding on the degree of cooperation. The level of trust will determine the price for, and provide a clear understanding of the consequences of, a decision for or against, cooperation.

In November 2012, the EU Ministers of Defence agreed to place cyber defence on the Pooling and Sharing agenda. With this principle of pooling and sharing, the EDA has established a framework for achieving more together without losing sovereignty over assets and resources. And projects in the areas of cyber defence training, exercise ranges, and cyber situation awareness packages for headquarters are reaching the end of the project preparation phase. More initiatives are currently under preparation.

Civil-military cooperation in the EU

In order to reduce the advantage of attackers, the current threat environment calls for very close civil-military cooperation. The EU rightly prides itself on its ability to deploy civilian and military responses to global crises. It is important that the EU adopts a common civilian and military approach to self-protection in cyberspace.

In this respect, the EU is in a good position with its “comprehensive approach” in security and defence. It combines responsibilities for both civil and military tasks under one roof. CSDP operations and missions by default claim close civil-military cooperation and interoperability. Consequently, the EU offers a natural harbour for close civil-military cooperation in cybersecurity and cyber defence. For instance, many defensive capabilities developed for cyberspace, either on the civil or the military side, have dual-use potential. And in order to be ahead of the threat wave, there is a need to exploit this potential for synergies and innovative solutions to the greatest extent possible. Thus, at the moment the EU is exploring how capabilities with dual-use potential could be developed under the EU structural and investment funds programme as well as how future CSDP-related research can be funded under future research framework programmes starting from 2021. In order to investigate this option, a preparatory action for CSDP-related research is currently under preparation. And in all these efforts, cybersecurity and defence are high on the agenda.

In addition, especially in times of financial austerity, it is important to ensure that all budgets are used in the most efficient way. The Project Team Cyber Defence in the EDA was established for example in such a comprehensive way.

Military networks, both classified and unclassified, depend on common Internet and network technology – the same hardware and software used by the civil side for their information infrastructures. To protect them the military must 'do' cybersecurity and use civilian standards. There are many common aspects of civilian and military cyber self-protection. EU military operations have a high dependence on civilian actors. In order to execute operations successfully, effective engagement at the unclassified/Internet level is essential. There is no difference between military and civilian actors in this area. To deliver effective protection, the military must be part of the civilian cyber protection activity and be able to share information with all actors and vice versa.

Just as EU Member States strive to ensure that government and national critical infrastructure within the EU are resilient to cyber threats, the equipment and systems deployed on EU-led CSDP operations and missions outside of the EU require at minimum the same level of protection.

Cooperation between NATO and the EU

22 nations are members of both the EU and NATO and each of these nations has a "single set of forces" available to serve on operations. In today's world these EU Member States cannot, and will not, invest in capabilities that can only be used by one organisation. The EU and NATO have therefore started to develop a dialogue in areas of common interest, such as converging NATO and EU standards in cybersecurity and defence. However, this engagement must be intensified. Furthermore, negotiations are on-going for an information-sharing framework between the NATO Computer Incident

Response Capability (NCIRC) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU).

The EU Cyber Security Strategy and its relationship with national cybersecurity strategies of EU Member States

Most EU Member States now have national cybersecurity strategies in place (although some were developed before the launch of the EU Cyber Security Strategy and some afterwards). ENISA has established an overview of existing strategies and their current status.[10] The challenge however is to ensure consistency between the different national strategies of the EU Member States and the EU Cyber Security Strategy itself. Although this EU strategy does not have a binding character like, for example, EU legislation such as Regulations and Directives, contradictions and ambiguities should be avoided. The EU has for such purposes, independent from the subject established, mechanisms in place which generally apply for legislative proposals but which are also used for strategic documents. This so called "Trialogue" between the European Commission, the Council of the European Union, and the European Parliament allows all stakeholders to contribute, comment, or provide interpretation on the respective document.

From a military perspective, the national cybersecurity strategies of EU Member States can be divided into two major types:

1. The first type are strategies that closely integrate civil and military capabilities. Such strategies occur in nations that traditionally use the concept of "total defence" like Scandinavian or Baltic states. In these strategies, the overall lead is often allocated directly to the government leader's cabinet.
2. The second type are strategies that have perhaps more loose coordination mechanisms for coordination between the military and the civil side. Such strategies are developed in countries that traditionally have a very strict separation between the civil governmental authorities and

military authorities. These strategies tend to define at a high level the responsibilities for the armed forces to protect their networks and include a seat in the national cybersecurity coordination centre, but often allocate the overall lead for national cybersecurity to the Minister of the Interior.

Nevertheless, there is no one-size-fits-all recipe for cybersecurity strategies. The strategy should reflect the national governmental and administrative traditions so that all the stakeholders feel comfortable. However, some key elements that should be addressed include the following:

- The strategy should address the national level of ambition in cyberspace and cybersecurity and it should integrate the views of all governmental areas and stakeholders;
- The engagement of academia, industry and citizen representatives should be ensured;
- Cross-border coordination and cooperation with third parties like other countries and inter- and supranational organisations like the UN, OSCE, EU or NATO should be addressed as the threat is global;
- The strategy must be augmented with sub-strategies, concepts and doctrine for all strategic sectors addressed;
- And finally, such a strategy has to be a living document since it must be adapted to reflect the rapid evolution of the threat as well as technological development.

Lastly, in order to support the development and maintenance of national cybersecurity strategies in EU Member States, ENISA has developed a guide for the development and implementation of national cybersecurity strategies.[11]

Conclusions

The public perception is that cyber protection is primarily a technological rather than human issue. However, technology is moving quickly to remove technical vulnerabilities and human factors are rapidly emerging as the priority, thus displacing technological issues.

For once technology is unlikely to be a significant issue in terms of military cyber defence. The synergies with civilian cyber defence ensures a constant stream of technology that will be used by military and civilian defenders to counter identical, or very similar, threats. The catch is the cyber defenders. In addition, the military are unlikely to have unique cyber defence capabilities, so they will be in direct competition with the civil side for personnel.

Following the findings of the EDA landscaping study, the EU placed emphasis on human factors in cyber defence - behind every cyber attack is an astute mind. For the time being, humans are our first (users) and our last (cyber defence specialists) lines of defence. For both attackers and defenders, the technology is the means with which they try to fulfil their objectives and achieve their aims. In that sense, there is no difference between the cyber and physical domains.

A challenge for the military, both today and in the future, will be growing and retaining sufficient high quality cyber trained people in our armed forces. While the cybersecurity technology market is broad and developing, the pool of young cyber talent with potential to become cyber specialists is small. In this competitive market, the military must find new and innovative ways to make the military an attractive option for talented individuals if we are to have the right people.

Moreover, the challenge is not limited to cyber specialists. All personnel, at all levels, require an increasingly sophisticated understanding of cyberspace and how to operate effectively in cyberspace. ICT users today - that is almost everybody in an organisation - have a role to play in cyber defence. Therefore, they must have up to date knowledge and awareness of the threat environment and how to react in the event of an incident. Furthermore, decision-makers must understand cyber options and the impact of cyber operations. A focus on cyber defence during education, training and exercises is consequently vital if we are to achieve an adequate operational cyber defence capability.

The human being is, and will continue to be, our most precious cyber defence asset. The knowledge and expertise of our people connected through well-developed processes and procedures is a fundamental requirement for a European cyber defence culture that enables acceptable operational capability in today's technological epoch.

Cybersecurity and defence call for close cooperation, whether at national level between the different governmental sectors, or in a whole-of-society approach between the public sector, citizens, private sector and academia, or in a wider sense at bilateral and multilateral level in the international environment.

The EU, both at national level within EU Member States as well as at Union level, has approached the challenges of cybersecurity in a comprehensive manner. This also includes the more recent developments relating to the countering of hybrid threats, where a reasonable cyber dimension can be assumed. Although the history of the military dimension of cybersecurity, in other words cyber defence in the EU in the context of CSDP, is still short, active measures are taken in a "whole-of-union" approach to make current and future CSDP operations more cyber resilient.

---

[1] **Disclaimer:** The views in this article are the author's own and do not represent the opinions of the European Defence Agency.

[2] Beyond own, organic defence and protection of EU institutions', bodies' and agencies' own ICT infrastructures.

[3] European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, JOIN(2013) 1 final, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, 7 February 2013. In fact, this was the first joint publication of the European Commission and European External Action Service (EEAS).

[4] European Council, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140214.pdf, Brussels, 19-20 December 2013.

[5] Council of the European Union, EU Cyber Defence Policy Framework, 15585/14, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf, 18 November 2014.

[6] RAND Europe et al, "Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)", Unclassified Summary, Prepared for the European Defence Agency

(CAP.10.111.2012) RR-286-EDA, http://www.rand.org/pubs/research_reports/RR286.html, March 2013.

[7] This understanding drove the revision of the CDP in 2014.

[8] EU Concept for Cyber Defence for EU-led Military Operations, December 2012 (not public).

[9] EU Cyber Defence Capability Requirements Statement, March 2013 (not public).

[10] ENISA, "National Cyber Security Strategies in the World", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

[11] ENISA, "National Cyber Security Strategies: An Implementation Guide", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Cybersecurity and Cybercrime: Philippine Perspectives and Strategies

Cybersecurity and Cybercrime: Philippine Perspectives and Strategies

Geronimo L. Sy, Assistant Secretary and Head, Office of Cybercrime, Department of Justice

This article outlines the cybersecurity and cybercrime landscape in the Philippines. It presents a framework analysis and highlights the country's most significant challenges and threats. It then explores national and local developments and discusses possible implications in the near and medium term.

Framework analysis

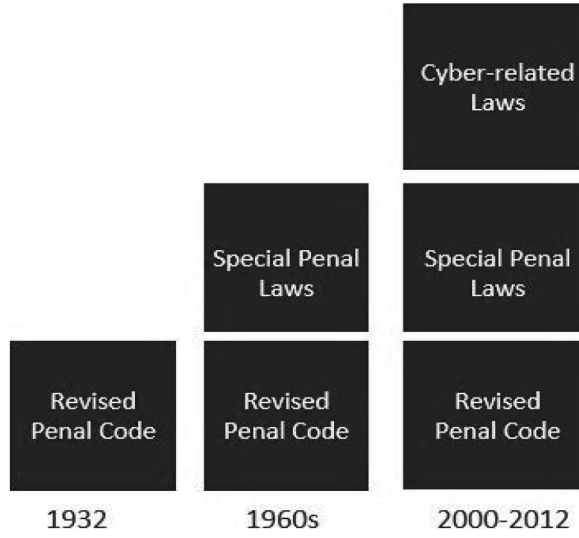
Cybersecurity and cybercrime are interrelated but may be distinguished in the context of law. Cybersecurity relates to the assurance of confidentiality, integrity, and availability of computer data and information and communications system. Whereas cybercrime is a subset of penal law that punishes crimes committed with the use of computer systems or where the system itself is the target. The fact that cybercrime is technology-related does not take it out of the operation of criminal law and procedure.

There is a classic tension between state protection of itself and the exercise of the rights of citizens under the rubric of civil liberties. The more expansive the rights, the more constraints there are on the state to act (and vice versa). In relation to cybersecurity and cybercrime, a broad approach to cybersecurity may narrow the scope of cybercrime (and vice versa).

In the Philippines, the general Revised Penal Code (RPC) was enacted in 1932, to codify punishable crimes.[1] In the intervening decades, amendments were made but the trend was to pass special penal laws in addition to the RPC to punish specific acts in response to emerging issues. The increase

of technology-driven laws came with the rise of Internet technology. The first such seminal law, the Electronic Commerce Act of 2000, was enacted shortly after the proliferation of the "I love you" virus of the same year in order to criminalise hacking.

The graph below illustrates the development of these laws:



Technology-related laws now include the following:

(1) The Special Protection of Children against Abuse, Exploitation and Discrimination Act;[2]
(2) The Access Devices Regulation Act of 1998;[3]
(3) The Electronic Commerce Act of 2000;[4]
(4) The Anti-Trafficking in Persons Act of 2003;[5]
(5) The Anti-Violence against Women and Children Act of 2004;[6]
(6) The Anti-Photo and Video Voyeurism Act of 2009;[7]
(7) The Anti-Child Pornography Act of 2009;[8]
(8) The Data Privacy Act of 2012 (Data Privacy Law);[9] and
(9) The Cybercrime Prevention Act of 2012 (Cybercrime Law)[10]

The Philippine National Security Policy for the period 2011 to 2016 identified cyber attacks as a security issue given that they may lead to a paralysis of communication infrastructure, international financial systems, critical government services and defence or military command and control systems.[11]

The Data Privacy Law was enacted to protect individual personal information in ICT systems in both the government and private sectors. It created the National Privacy Commission to administer and implement the provisions of the law, as well as monitor and ensure compliance with international data protection standards. Its salient provisions include: (1) the scope or types of information covered by the law;[12] (2) sanctions on the unauthorised processing, access, and/or disposal of personal, privileged, and/or sensitive personal information;[13] and (3) exceptions to the unauthorised processing of information.[14]

In September 2012, the Cybercrime Law was approved as the first comprehensive legislation on cybercrimes. Notably, it defines "cybersecurity" as the "application of security measures to ensure confidentiality, integrity, and availability of data. It is a collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization, as well as a user's assets."[15] This differs from the usual practice in the Philippines of defining cybersecurity in executive pronouncements, and there is no equivalent definition of cybercrime.[16] This law established the Office of Cybercrime under the Department of Justice (DOJ-OOC), which is designated as the central authority in all matters related to international mutual assistance and extradition. In addition, to enhance enforcement and implementation, specialised cybercrime units were designated to be manned by dedicated investigators in the Philippine National Police and the National Bureau of Investigation.

The Cybercrime Investigation and Coordinating Center (CICC) was also created pursuant to the Cybercrime Law. The CICC is an inter-agency body under the administrative supervision of the Office of the President that

coordinates policies among concerned agencies. It is tasked to formulate and enforce the national cybersecurity plan and to extend immediate assistance in real time for cybercrime offences through a computer emergency response team.[17]

However, the Cybercrime Law was challenged by 15 petitions in the Supreme Court. The main grounds were the constitutionality of: (1) the provisions of certain acts as crimes and the imposition of penalties for their commission; (2) provisions that would enable the Government to track down and penalise violators; and (3) online libel in relation to related articles of the RPC. Nevertheless, in 2014, the Supreme Court, in the case Disini-v-Secretary of Justice,[18] upheld the constitutionality of the law. The court found that there are sufficient standards for the CICC to follow when it provided a definition of "cybersecurity".[19] However three provisions were declared void, namely posting unsolicited commercial communications, collecting traffic data in real-time, and blocking access to suspicious computer data.

There are three core cybercrimes under the law: (1) Offences against the confidentiality, integrity and availability of computer data and systems; (2) Computer-related offences; and (3) Content-related offences. Of note, penalties are increased for the first class of cybercrime if committed against critical infrastructures.[20] In addition, this first class of core cybercrimes may be said to apply to cybersecurity and data privacy. The second class may also apply, particularly the act of identity theft as its subject is personal information.

There is no separate class of cybersecurity crimes but rather cybercrimes that deal with the issue of cybersecurity. Among these crimes, the priorities of the DOJ-OOC are online child abuse, online fraud, and network security.

Challenges and threats

The main challenge to implementing cybersecurity and cybercrime regulation is the need for effective enforcement.

With the newly created designated focal units, there are now offices responsible for both cybersecurity and cybercrime. The next step is to provide rules and regulations to clarify the legal provisions and to "fill in the gaps". Advisories and circulars are also needed to guide the public and specific sectors, especially those in the field of technology. In addition, there is a continuous need for capacity-building relating to personnel so they can understand the technology as well as the law. While investigators, prosecutors, public defence lawyers, and judges may be well versed in criminal law and procedure, they may not have the requisite skills for handling cyber issues and electronic evidence.

Another significant challenge is the balancing of state and individual rights discussed earlier. While the standards of individual liberties are set, the intersection of cybersecurity and cybercrime and their impact on rights is an evolving matter.

These issues arise in the context of a changing cybersecurity and cybercrime landscape with new technologies and disruptions caused by innovation. Technologies develop at a very fast pace whereas legislation requires time to adapt. Furthermore, by their nature, it is difficult to measure the success or impact of cyber measures.

Recent developments

a) Specialised and coordinating units:
To improve the fight against cybercrime, a National Prosecution Task Force on Cybercrime was established in September 2014 to handle cybercrime cases. The Cybercrime Desk, which handles Mutual Legal Assistance and Extradition requests, was then set up. It serves as the contact point in the DOJ for international legal cooperation involving cybercrime and related matters.

The DOJ established a Cyber Security Incident Response Team (DOJ-CSIRT) in May 2015, which is a multi-disciplinary group that covers relevant

offices under the Department, headed by its DOJ Chief Information Officer. Its duties and responsibilities are to: (1) Respond and extend immediate assistance to the concerned agency on cybersecurity incidents; (2) Issue and promulgate guidelines, advisories, and procedures in all matters related to cybersecurity, in accordance with the national cybersecurity plan; (3) Conduct cybersecurity training and awareness; and (4) Ensure proper coordination among DOJ constituents, attached agencies, and other relevant sectors in the preparation of appropriate and effective measures to strengthen the cybersecurity capabilities of the Department against cyber threats.

A Sub-Committee on Cybercrime was also established by the National Law Enforcement Coordinating Committee (NALECC), and the DOJ-OOC is designated Chair.[21] It comprises 24 founding member agencies and is mandated to; 1) provide assistance in the anti-cybercrime campaign to other government agencies, the private sector and NGOs (such as facilitating information-sharing and the arrest of those involved in cybercrime); 2) to strengthen inter-agency coordination relating to anti-cybercrime and other cybercrime-related activities; and 3) to provide a venue for discussion and recommendations on issues that affect the anti-cybercrime campaign of the Sub-Committee member agency.

b) Capacity building programs:

In 2014, the United Nations Office on Drugs and Crime (UNODC) partnered with DOJ-OOC to provide training to law enforcement officials and prosecutors. Through the training, prosecutors acquired skills and knowledge to support cybercrime investigations from the stage of initial reports to the preparation of prosecution case papers.

The DOJ-OOC continuously provides a technical and legal framework to combat cybercrime and aims to develop systematic law enforcement in line with international best practices. Eight of the 18 regions in the country were covered under the first year of training programs. The basic cybercrime investigation training covered first responders training and procedures in cybercrime investigations; handling and analysing electronic and digital

evidence; cyber incident response; and digital forensics. These training sessions involved more than 500 individuals, including investigators, prosecutors, state counsels, and public attorneys. Likewise, the DOJ-OOC was able to train trial judges and appellate justices on cybercrime cases, in partnership with the Philippine Supreme Court and the Council of Europe. The "cybercrime judges" were also trained to serve as trainers so as to then share and multiply their acquired learning with colleagues, in other words "training the trainer".

c) Partnerships:

In all cybercrime investigations, computer forensics is mostly, if not always, at the heart of such investigations. It is a complicated science with its own history, implications, and future. In light of this, a National Computer Forensics Training Program will be launched to train law enforcement in computer forensics and provide structured procedures and guidelines consistent with international best practices. For this training, the DOJ-OOC has had initial discussions with key partners who will provide international specialists to share their knowledge and expertise with law enforcement authorities.

To further enhance investigations, the DOJ-OOC was introduced to INTERPOL's International Child Sexual Exploitation (ICSA) image database. This database allows for the extracting of digital information from images to check against existing data, and it has numerous other features designed to aid investigators. It is expected that the DOJ-OOC will have access to the database in 2016. In line with the commitment of the Philippines to the Global Alliance against Child Sexual Abuse, the Convergence of Councils and Committees for Child Protection held a roundtable dialogue with public and private stakeholders to discuss areas of cooperation and partnerships in order to intensify the fight against the alarming increase in the number of cases of abuse and exploitation of children online. Advocacy, prevention, and protection groups were formed, comprising representatives from different government agencies and private stakeholders.

d) Regulations:

The Implementing Rules and Regulations (IRR) of the Cybercrime Law was signed by the Departments of Justice, Interior and Local Government, and Science and Technology in August 2015. It contains the details and mechanics on the implementation of the cybercrime law. The IRR went through a series of government and public consultations that included stakeholders from business, academia, NGOs, the legal profession, media, ICT groups and Internet service providers.

The National Telecommunications Commission recently released a memorandum circular providing for guidelines on blocking or filtering technologies to block access to all websites carrying child pornography materials. This mandates service providers to install such technologies in compliance with the Anti-Child Pornography law.

Lastly, the DOJ-OOC in its focus on crime prevention issued advisories on sextortion, online shopping fraud, and online child abuse. It is also due to publish a primer on cybercrime laws, rules and regulations, as well as an investigation manual to guide citizens and law enforcement officers.

Conclusion

The Philippines was invited to accede to the Convention on Cybercrime in 2011 (the country became an observer to the Cybercrime Convention Committee (T-CY) in 2010). The ratification process is underway and the Philippines is expected to accede to the Convention in the near to medium term for the next stage of strategies on cybersecurity and cybercrime.

---

[1] Act No. 3815, the Revised Penal Code of the Philippines (1932).
[2] Republic Act (R.A.) 7610 (1992).
[3] R.A. 8484 (1998).
[4] R.A. 8792 (2000).
[5] R.A. 9208 (2003).
[6] R.A. 9262 (2004).
[7] R.A. 9995 (2009).

[8] R.A. 9775 (2009).
[9] R.A. 10173 (2012).
[10] R.A. 10175 (2012).
[11] Official Gazette, National Security Policy (2011-2016), Securing the Gains of Democracy, Republic of the Philippines, http://www.nsc.gov.ph/attachments/article/29/NSP-2011-2016.pdf.
[12] Section 4 of R.A. 10173 (2012) or the "Data Privacy Act of 2012" (DPA).
[13] Sections 25-33 of the DPA.
[14] Section 13 of the DPA.
[15] Section 3 (k) of Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012" (CPA).
[16] Section 3 of the CPA.
[17] Section 24 and 26 of the CPA.
[18] G.R. No. 203335, 11 February 2014, Disini vs. Secretary of Justice.
[19] G.R. No. 203335, 11 February 2014, Disini vs. Secretary of Justice.
[20] Section 8 of the CPA;
Section 3 (j) of the CPA defines "critical infrastructures" as computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to the country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.
[21] NALECC was established pursuant to Executive Order No. 829, as amended by E.O. No. 41 dated 9 December 1992, to serve as the venue for the coordination of all enforcement activities of various government law enforcement agencies.

Cybersecurity Trends and Issues: A Singapore Perspective

Cybersecurity Trends and Issues: A Singapore Perspective

John Yong, Director, Infocomm Security Group, Infocomm Development Authority of Singapore

Singapore is a small island with a big dream in information and communication technologies (ICT). The Infocomm Development Authority (IDA), which is a statutory board of the Ministry of Communications and Information (MCI), is chartered to conduct the following for Singapore: 1) Enable business innovation and transformation; 2) Strategise and implement e-Government; and 3) Empower society to leverage ICT to enrich lives.

First, in order to enable business innovation and transformation, IDA promotes the adoption of infocomm technology as a key enabler to enhance Singapore's economic competitiveness. It works with both public and private organisations to spearhead the strategic use of infocomm in various sectors such as education, healthcare, manufacturing, logistics, tourism, transport, entertainment and finance. Second, in relation to strategising and implementing e-Government, IDA (as the Chief Information Officer for the Singapore government) is responsible for master plans, project management, and the implementation of various infocomm systems and capabilities for the Government. It oversees IT standards, policies, guidelines and procedures for the Government, and manages the information security of critical infocomm infrastructure. Third, to empower society to leverage infocomm so as to enrich lives, IDA seeks to build a digitally inclusive society where lives are enriched by infocomm. IDA works with industry partners and associations to encourage all segments of society to adopt infocomm and use it in a more sophisticated way. This includes providing assistance to low-income households, senior citizens, and people with disabilities so they may acquire computers and become connected to the Internet. IDA also works with community organisations to develop applications that help these organisations reach out to their members and constituents.

“Smart Nation”

One of the latest developments in Singapore is the country’s ambition to transform the Singapore city state into a “smart nation”. In November 2014, the Prime Minister described this idea of a smart nation and the country’s vision to be a smart nation as a nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all.

There are numerous reasons why Singapore holds this ambition. The nation must address several challenges to ensure that it is well positioned for the future. First, Singapore has a very high density as a city. By way of comparison, in the United States and South Korea, there are approximately 35 and 500 people per square kilometre respectively whereas in Singapore there are 8,000 people per square kilometre. Second, the country has an ageing population and the number of people aged 65 plus is expected to triple to 900,000 by 2030. Third, Singaporeans and those living in this part of the world enjoy technology. We see this as an opportunity to explore what technology today can do to create better living, opportunities and stronger communities in our society. There may be 5 million people living in Singapore, but in the digital realm this city state manages billions, if not trillions, of user accounts. The digital (electronic) population, in other words the e-citizens, managed in Singapore is probably beyond imagination and there is a desire to understand how digital data could change the way we analyse various trends and phenomena to derive answers and insights for complex questions.

Other considerations

Hardware is going to become a commodity. For people living in the fifties or sixties, hardware was limited to only those who could afford it. Today, most households now have multiple televisions. Likewise, computing resources are fast becoming a commodity today. In recent months, many discussions have focused on the Internet of Things (IoT) - if you understand the desire

of the city state and users, a likely future trend will be commoditisation of the hardware; understanding big data; and translating it into useful citizen applications for success.

This is all linked to IoT. Although IoT may mean different things to different people: gamers use it for enjoyment purposes; and the medical field uses IoT to track patients' critical medical conditions. Nevertheless, IoT is not safe unless we develop and build it properly. In addition, when it comes to giving citizens high Internet bandwidth, Singapore operators charge households about USD40 for one gigabytes per second Internet bandwidth (possibly one of the cheapest rates globally).

Smart initiatives

At this juncture, several smart initiatives are being developed by various communities. These include, among others, autonomous vehicles, smart homes (life at home becomes more efficient through IoT and ICT), smart dispensary system, crowdsourcing, Internet for the public, ubiquitous Wi-Fi, smart transport, and smart medical care.

Stay competitive

As a city state, Singapore needs to stay relevant and competitive by finding new ways to do so. For example, a banker in one of the largest banks in Singapore described this by saying two things: First, whether we know it or not, the digital revolution has put banks under siege. With Internet 2.0 and mobility, the game has been re-defined. Banks in Asia are on a burning platform of competition from mobile and internet companies. If we do not embrace digital – and quickly – there is a real danger that our lunch will be eaten. After elaborating the digital impact on the bank, he added: The good news is I do not believe any bank in Asia has had massive success around digital banking. This gives us a window to turn challenge into opportunity.

It is a very important development that some of the economies are transforming. This means that ICT is going to be deployed in the city state to its fullest potential in order to achieve new ways to compete and therefore transform.

Risks

There are two major risks arising with the smart nation vision. First, there are data privacy concerns since citizen privacy needs to be protected given that data is collected by various systems. These systems are complex. A system could mean a sensor, an operator system, government systems, or any device that can hold data. Second, the cybersecurity threat is becoming more frequent, much more sophisticated, and much more targeted towards the Government and businesses. While many reports assert that the number of cybersecurity incidents has grown tremendously over the past few years, what about those that have not been reported by firms? Is there a higher percentage? It is likely that that in every ten cases, firms will only report one, in which case we most likely only see the tip of the iceberg.

Cybersecurity is worrisome, especially the "3 Ds": defacement, disruption, and data breach. Citizens and users demand cybersecurity protection - they expect 99.99% but the resilience of most systems is only 99.5% or lower. This means that disruption is unacceptable. And in terms of data breaches, this could impact the organisation. Moreover, the country cannot allow reputational damage. Singapore is also concerned about corporate industrial espionage as well as financial losses.

Consequently, we need to have a sufficient cybersecurity budget in order to achieve the minimum level of system hygiene and this could be anything between four and eight per cent of the ICT system budget. Thus the Minister for Information and Communications, Yaacob bin Ibrahim, recently said that up to ten per cent of Singapore's information technology budget will be spent on cybersecurity and the Government is urging private companies to do

likewise. For many of the incidents over recent months, they do not seem to be accidental and statistics suggest that this has also become more frequent. It is important therefore that the cybersecurity threat not be underestimated, and that it is addressed carefully.

Mitigating measures

We are doing a number of things in order to address this cybersecurity threat landscape. The standard cybersecurity lifecycle is often known as prevent, detect, and recover, which the author understands as T-1, T=0, T+1. T-1 means you must practice predicting what might go wrong so that it can be addressed quickly and mitigated in line with your plan. T=0 means when something happens, you need to know very quickly. This should be known immediately - if not within minutes or hours. However this is a very difficult objective to achieve. Lastly, T+1 - things always happen. It is hard to think of an organisation or city state that has never had a cybersecurity attack. It is important therefore to have in place a measure so that the system can be restored; what is happening can be understood; and hopefully the same mistake will not be repeated.

And while it seems like a battle between us and the adversary, and we always think that the adversary learns faster than us, the truth is that we also have very clever people on the right side. By way of example, at a recent RSA event in the United States, Ed Giorgio on the Cryptographers' Panel 2015 mentioned that the code maker side needs 1,700 people, whereas the code breaker side only needs 17. So to deal with one hacker, 100 people are needed. This balance clearly needs to shift and we need to know how to deal with this problem.

IDA's initiatives

The Singapore government has done several things to protect the Government and telecomm industry. First, a new Code of Practice, part of the Singapore Telecom Act, was launched to allow the regulator to exercise greater power over the ISPs/operators for cybersecurity protection. The aim is that operators be able to handle DDOS attacks themselves, and hence, able to provide for enterprise downstream.

Second, the Government has appointed a Ministry Chief Information Security Officer (MCISO) at IDA level, and established an Ops and Command Centre (MOCC). This allows IDA to have greater control over cyber incidents so that it can know what to do quickly. Analytical skills have also been improved through collaboration among various government agencies.

Conclusion

To conclude, first, as CISO, can you handle the 3Ds; do you have the T-1, T=0 and T+1 capabilities; and a maturity index against which cybersecurity protection can be mapped? Second, can security by design be built within ICT or sophisticated ICT systems. This is not easy because there are always things that cannot be put into the design. Is security pervasive and adaptive enough? There is a certain amount of intelligence built into adaptiveness and it is important to learn from each other as to how cybersecurity can be made more pervasive and adaptive.

Finally, the importance of collaboration in cyber information sharing cannot be overestimated. It is important to stay in tune with the greater community to share and learn from each other. For instance, a recent bill passed by U.S. Congress encourages information sharing to a greater degree. At the enterprise level, some form of safe harbour policy may need to be considered to ensure enterprises will not be implicated if they share data with another party.

SOURCES

https://www.ida.gov.sg/About-Us/What-We-Do

http://www.pmo.gov.sg/mediacentre/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november

http://www.dbs.com/newsroom/influencer/default.page

http://www.straitstimes.com/world/europe/smart-nation-vision-about-people-and-mindsets-vivian

http://www.gov.sg/news/content/the-straits-times-spore-to-spend-10-of-it-budget-on-cyber-security

http://www.rsaconference.com/videos/the-cryptographers-panel-2015

Contributors' Biographies

Contributors' Biographies

Daniel Castro
Vice President, Information Technology & Innovation Foundation

Daniel Castro is the Vice President of the Information Technology and Innovation Foundation and Director of the Center for Data Innovation. Daniel writes and speaks on a variety of issues related to information technology and Internet policy, including privacy, security, intellectual property, Internet governance, e-government, and accessibility for people with disabilities. His work has been quoted and cited in numerous media outlets, including The Washington Post, The Wall Street Journal, NPR, USA Today, Bloomberg News, and Businessweek. In 2013, Mr. Castro was named to FedScoop's list of "Top 25 most influential people under 40 in government and tech." In 2015, U.S. Secretary of Commerce Penny Pritzker appointed Danielto the Commerce Data Advisory Council.

Before joining ITIF, Daniel worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He contributed to GAO reports on the state of information security at a variety of federal agencies, including the Securities and Exchange Commission (SEC) and the Federal Deposit Insurance Corporation (FDIC). In addition, Daniel was a Visiting Scientist at the Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania where he developed virtual training simulations to provide clients with hands-on training of the latest information security tools. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Simon Chesterman
Dean, Faculty of Law, National University of Singapore

Professor Simon Chesterman is Dean of the National University of Singapore Faculty of Law. He is also Editor of the Asian Journal of International Law and Secretary-General of the Asian Society of International Law.

Educated in Melbourne, Beijing, Amsterdam, and Oxford, Simon's teaching experience includes periods at the Universities of Melbourne, Oxford, Southampton, Columbia, and Sciences Po. From 2006-2011, he was Global Professor and Director of the New York University School of Law Singapore Programme.

Prior to joining NYU, Simon was a Senior Associate at the International Peace Academy and Director of UN Relations at the International Crisis Group in New York. He has previously worked for the UN Office for the Coordination of Humanitarian Affairs in Yugoslavia and interned at the International Criminal Tribunal for Rwanda.

Simon is the author or editor of twelve books, including One Nation Under Surveillance (OUP, 2011); Law and Practice of the United Nations (with Thomas M. Franck and David M. Malone, OUP, 2008); You, The People (OUP, 2004); and Just War or Just Peace? (OUP, 2001). He is a recognised authority on international law, whose work has opened up new areas of research on conceptions of public authority - including the rules and institutions of global governance, state-building and post-conflict reconstruction, and the changing role of intelligence agencies.

Bryan Tan
Partner, Pinsent Masons MPillay LLP, Singapore

Bryan Tan is a Singapore-qualified lawyer and has led many industry firsts including the first mass e-mail defamation case in the world, Singapore's

first publicised telecoms competition dispute, a pan-Asian co-branded travel portal, the first privately-funded cable landing project in Singapore, and the world's first registrar-level domain name dispute. Since 2004, Bryan is also named one of the leading individuals in IP, IT and telecoms law by Best Lawyers, Chambers, Legal500, Who's Who and AsiaLaw. He is a partner at international law firm Pinsent Masons.

Bryan represents major Internet and software companies as well as governments and government entities. He has also been a member of the Media Literacy Council, Law Society's Information Technology and International Relations sub-committees, as well as the LawNet Management Committee. He sits on the audit committee of the Singapore Training and Development Association and the board of directors of the YMCA of Singapore, the Internet Society Singapore chapter and the Council of the National Youth Achievement Award (Duke of Edinburgh's Award). Bryan is an author of Halsbury's Laws of Singapore - E-Commerce and Halsbury's Laws of Malaysia - E-Commerce (both editions). He also co-wrote the Singapore chapter of Electronic Evidence (three editions) with Prof. Daniel Seng, the practitioner's chapter on Data Protection Law in Singapore and the Singapore chapter on The Comparative Law of Higher Education. For the last six years, Bryan has also been a legal advisor to the ASEAN Single Window project.

Michael Mylrea

Manager for Cybersecurity and Energy Infrastructure, Pacific Northwest National Laboratory. National Science Foundation: Executive Cyber Security Doctoral Fellow, George Washington University

Michael Mylrea is a Chief Information Security Officer with over a decade of experience working on cybersecurity, energy and national security issues in various research, technical and policy capacities. This experience includes diverse clients and employment in government and industry, including, but not limited to: Department of Energy, Deloitte, U.S. Department of Defense,

U.S. Cyber Consequences Unit (Director for Energy), Lakeside Oil, MIT Lincoln Lab, Harvard Berkman Center, and Good Harbor Consulting (Senior Advisor to Richard A. Clarke). His cybersecurity thought leadership has appeared in news and journal articles, television, congressional testimony and is frequently cited in industry and government publications. Upcoming publications include a cyber-energy study with Sandia National Lab, a book on cybersecurity leadership and research on smart building cyber security optimisation at Stanford University. Michael is also a National Science Foundation, Executive Cyber Security Fellow pursuing a doctorate at George Washington University.

Michael received a Master's degree from The Fletcher School at Tufts University and enrolled in credited course work at Harvard Law School and Kennedy School of Government. He received two BAs from University of Wisconsin-Madison. Michael is a recipient of a Fulbright Scholarship and is proficient in Hebrew, Arabic and Spanish.

Yono Reksoprodjo

Lecturer and Researcher on Asymmetric Strategy Studies, Indonesia Defense University – (UNHAN)

Dr. Yono Reksoprodjo graduated as a Naval Architect from the Faculty of Technology, University of Indonesia in 1987. He pursued his DPhil in Computer Aided Engineering Systems with emphasis on Reverse Engineering Technology from Imperial College, University of London in the UK in 1994.

Yono sits as an Expert Staff to the National Desk for Information Resilience and Cyber Security, at the Coordinating Ministry for Politics, Legal & Security Affairs in Indonesia and, is the Vice President of Corporate Affairs and Development of Sintesa Group. He lectures at the Indonesian Defense University (UNHAN).

Jason Healey

Senior Research Scholar, Columbia University's School of International and Public Affairs

Jason Healey is a Senior Research Scholar at Columbia University's School for International and Public Affairs specialising in cyber conflict, competition and cooperation. Prior to this, he was the founding director of the Cyber Statecraft Initiative of the Atlantic Council where he remains a Senior Fellow. He is the author of dozens of published articles and the editor of the first history of conflict in cyberspace, A Fierce Domain: Cyber Conflict, 1986 to 2012.

During Jason's time in the White House, he was a director for cyber policy and helped advise the President and coordinate U.S. efforts to secure U.S. cyberspace and critical infrastructure. He has also been executive director at Goldman Sachs in Hong Kong and New York, vice chairman of the FS-ISAC (the information sharing and security organisation for the finance sector) and a US Air Force intelligence officer having worked at the Pentagon and National Security Agency. Jason was a founding member (plankholder) of the first cyber command in the world, the Joint Task Force for Computer Network Defense, in 1998. He is president of the Cyber Conflict Studies Association, and has been a lecturer in cyber policy at Georgetown University and Johns Hopkins School of Advanced International Studies.

Zhu Qichao

Director and Professor of the Center for National Security and Strategic Studies (CNSSS), National University of Defense Technology, China

Dr. ZHU Qichao is the Director and Professor of the Center for National Security and Strategic Studies (CNSSS), National University of Defense Technology (NUDT). Prior to his current position, he was the deputy director of CNSSS from 2010 to 2012, and one of the assistant researchers of the Policy Analysis Center, NUDT, from 2007 to 2010. Qichao was a senior

visiting research fellow in the Department of War Studies, King's College London from September 2011 to March 2012.

Qichao's areas of expertise are cybersecurity, cross-domain security, technology and Revolution in Military Affairs. He has a B.A, a M.A., and a PhD (all NUDT). In recent years, he has been invited to give talks at the Sino-American Cyber Dialogue, the Sanya Initiative Dialogue, the Garmisch-Patenkirchen International Information Security Forum, and China Aerospace International Forum (AIF), among others.

William H Boothby
Air Commodore (Retired)

During a 30-year career in the RAF Legal Branch, Air Commodore Bill Boothby (Retired) served in the UK, Germany, Hong Kong, Cyprus and Croatia, retiring as Deputy Director of Legal Services in July 2011. In 2009 he took a Doctorate in International Law at the Europa Universität Viadrina, Frankfurt (Oder) in Germany. In the same year, he published 'Weapons and the Law of Armed Conflict' through OUP and his second book, 'The Law of Targeting', appeared with the same publisher in 2012. He was a member of the Group of Experts convened by the ICRC to discuss Direct Participation in Hostilities; a member of the Group of Experts who produced the HPCR Manual of the Law of Air and Missile Warfare; and a member of the Group of Experts as well as the drafting committee of the CCD COE project that produced the Tallinn Manual on the Law of Cyber Warfare.

He has an associate fellowship at the Geneva Centre for Security Policy and teaches at Royal Holloway College, University of London, King's College, University of London, and at the Australian National University, Canberra. His third book, addressing Conflict Law, was published in 2014. He lectures and speaks widely on international law issues.

Robert J. Butler
Senior Advisor to The Chertoff Group

Bob Butler is the co-founder and managing director of Cyber Strategies LLC. Previously, he served as the Chief Security Officer for IO, a global data center service and product firm. He has consulted as a Special Government Expert to the Office of the Secretary of Defense, Air Force Scientific Advisory Board and other organisations on cybersecurity and enterprise risk management. He also serves as a fellow at the Center for New American Security (CNAS) and is a member of the Texas State Cyber Security, Education and Economic Development Council. Prior to assuming his current roles, Bob served as the first Deputy Assistant Secretary of Defense for Cyber Policy (August 2009-August 2011.) In this role, he acted as the principal advisor to the Secretary of Defense and other Defense leaders on the development of cyber strategy and policy.

Bob has a distinguished career in information technology, intelligence, and national security that spans 34 years in both public and private sectors. He is a retired U.S. Air Force colonel and a former member of the Defense Department's Senior Executive Service. He has also been an account executive and senior cyber strategist with Computer Sciences Corporation.

He earned a Bachelor of Science degree in Computer Information Systems from Manhattan College and a Master of Business Administration from the School of Business at the University of Maryland. He is a former RAND fellow and has served as a National Defense Fellow at Georgetown University's School of Foreign Service. He has received a number of public service awards including the Armed Forces Communications Electronics Association's North America Information Technology Leadership award.

Wolfgang Röhrig
Programme Manager, Cyber Defence at the European Defence Agency

Wolfgang Röhrig is the Programme Manager Cyber Defence of the European Defence Agency (EDA). He was born in Germany and entered the German Navy in 1985. After completing his studies at the University of the Federal Armed Forces in Hamburg, with the MBA degree in 1990, he served in several officer positions in the German Navy and the German Joint Services (including several operational deployments and service in NATO).

Wolfgang bears the military rank of a German Navy Commander. He joined the EDA in 2012 as Project Officer and became programme manager cyber defence at the beginning of 2014. In his current position, he is responsible for the identification of capability gaps with respect to cyber defence in EU-led military operations, and the development and implementation of solutions for closing these gaps through cooperative projects with EU Member States.

Geronimo L. Sy
Assistant Secretary and Head, Office of Cybercrime, Department of Justice

Geronimo L. Sy is Assistant Secretary at the Philippine Department of Justice (DOJ) and head of the Office of Cybercrime (OOC). He serves as Chief Information Officer and Chairperson of the DOJ Cyber Security Incident Response Team. He is a member of the Supreme Court Committee on the Revision of the Rules of Court and E-Commerce.

Geronimo successfully prosecuted the first cybercrime cases in the country, and established the e-Government Task Force on Cybercrime and Cybersecurity in 2007. The leading Cybercrime Prevention Act of 2012 was the result of Geronimo's advocacy. His publications on the subject include *"*Justice Online: Issues and Solutions" *(World Crime Forum, 2013)* and *"*E-Commerce Act of the Philippines" *(Rex Publishing House, 2001)*. Geronimo is a Management

Engineering and Juris Doctor graduate of the Ateneo de Manila University. He earned his MA in Public Management from the University of the Philippines. At present, he is pursuing a Doctorate of Public Administration from the National College of Public Administration and Governance.

John Yong

Director, Infocomm Security Group, Infocomm Development Authority of Singapore

John Yong is Director, Infocomm Security Group, at the Infocomm Development Authority of Singapore (IDA). John holds a Masters in Computer Science from the University of Salford, United Kingdom. He is a seasoned infocomm security professional who has dedicated his 35-year career to this field, both in the public and private sectors.

John started his career with the Ministry of Defence before joining the then National Computer Board (NCB) in 1991 to head its IT Security Department. He then moved to the private sector and worked for a number of multinational corporations in various management and consulting roles. Prior to joining IDA, he served as Chief Security Advisor to a major Southeast Asian telecommunications group. In recognition of his achievements and contributions, John received the International Data Group (IDG) ASEAN Chief Security Officer (CSO) Awards and was honoured as one of the most outstanding Chief Security Officers in 2013.

About the Centre of Excellence for National Security (CENS)

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.

About the S. Rajaratnam School of International Studies (RSIS)

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 (NSCS)

The National Security Coordination Secretariat (NSCS) was set up in the Prime Minister's Office in July 2004 to facilitate national security policy coordination from a Whole-Of-Government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is Deputy Prime Minister and Minister for Home Affairs Mr Teo Chee Hean.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS (NSIC) is Mr Benny Lim, who is concurrently Permanent Secretary (National Development) and Permanent Secretary (Prime Minister's Office).

NSCS comprises two centres: the National Security Coordination Centre (NSCC) and the National Security Research Centre (NSRC). Each centre is headed by a Senior Director.

The agency performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipation of strategic threats. It also organises and manages national security programmes, one example being the Asia-Pacific Programme for Senior National Security Officers, and funds experimental, research or start-up projects that contribute to our national security.

For more information about NSCS, visit http://www.nscs.gov.sg/

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg