Cybersecurity

Some Critical Insights and Perspectives

Edited by
Damien D. Cheong

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

Cybersecurity
Some Critical Insights and Perspectives

Edited by:
Damien D. Cheong

Foreword

This collection of short commentaries looks at the on-going debates and issues that relate to cybersecurity, Internet governance and related strategies.

The authors include practitioners, researchers and academics.

We hope these commentaries prove informative, and that the reader will be able to derive some useful takeaways.

Table of Contents

Cybersecurity: The Strategic View

Cybersecurity: The Strategic View

Kah-Kin Ho

I'd like to start by giving everyone my own personal subjective assessment on the state of security capabilities of different enterprises around the globe. The good news is that the security capabilities of large enterprises relative to the growing sophistication of cyber-threats are growing steadily. However, the same cannot be said of small and medium enterprises, where over time, their relative capabilities are declining, and the gap between large and small medium enterprises is widening. This is hardly surprising when you look at the figures IT Security spend per head. With economies of scale, large enterprises can hire the best and brightest security experts, purchase the best security tools, and put in place a truly robust security program that is able to operationalise the use of intelligence to detect threats.

In a number of countries, large enterprises have close collaboration with their security services in threat intelligence sharing. This leaves smaller enterprises lagging behind both at the level of technology as well as cyber-intelligence foresight, and furthermore, they cannot afford the required talent to manage the complexity of the multi-dimensional problems that cyber-attacks present.

So what is the impact of these challenges on small businesses globally? As small and medium enterprises form the bedrock of most economies globally, this situation (lack of technology, talent and cyber-intelligence) is not sustainable in the long run. This holds true for such organisations as well as the relevant governments, which have such a high level of risk within their national GDP.

So what could be the solutions to this? I am inclined to believe that one key solution is for small and medium enterprises to outsource their security management to more capable organisations. Across the board, the use of cyber-insurance is going to be critical to lower their risk exposure and improve

cash flow management. One could argue that there is a role of government in this arena as the “reinsurer of last resort” to provide some level of stability and certainty to the market place.

Let us explore this “role” for governments in greater detail, and I would argue that this is of vital importance. It is important to start with the premise that for most governments globally, the 1980s, 1990s and 2000s signalled an era of wide-scale deregulation and privatisation, with much of the nation’s critical infrastructures – in sectors such as energy, transport, finance, medicine and so on – entrusted to the private sector.

Critical infrastructures are constantly targeted by cyber-adversaries, and we have seen security incidents exert both cascading and crippling effects regionally, nationally, and even internationally, due to the high degree of interconnectedness and interdependency that our global society now involves. So when we look at the cost of a security incident it is not just the private cost of say replacing a power generator but essentially there is the social cost component as well. We call this a security externality but it is a negative one because it adversely affects everyone else.

Part of the reason why it can be difficult to secure critical infrastructures is due to the divergence of interests between the private and public sectors. The private sector’s primary focus is corporate efficiency: in terms of security, it does what it believes is “enough”, implementing the bare minimum level of security, since its main goal is profit-making. The government, in contrast, is principally concerned with achieving social order, national security and economic prosperity for its population. In the EU for example, most citizens expect their governments to protect them from all hazards. Yet in this case, governments do not have supervisory and operational control over these critical infrastructures. Some people have argued that the role of government as the legitimate security provider has diminished and will continue to decline over time.

As I meet with different governing bodies around the world, I am of the opinion that this matter is not straightforward for them, and that they are indeed grappling with the challenge of determining what their role in cybersecurity could or should be, especially *vis-a-vis* the private sector. I argue, however, that the changing global landscape should not imply that the role of governments, as the legitimate provider of security, be diminished, provided they are able to understand clearly how the world has changed and is changing, and what their role should be within this new environment of increasing interconnectedness.

Furthermore, I argue that in order for governments to be successful in this new environment, their remit must transcend what their historical regulatory role has typically entailed. They now need to tackle the questions of how they can best assist the private sector to invest in security (facilitation), and how both the public and private sectors can improve the current state of security (collaboration). To formulate a viable approach, this is the framework through which governments must strategise, and they must be ready to draw upon analogous lessons learned from past preparedness efforts geared towards other areas of threat, such as pandemics and terrorism.

With regard to law enforcement, the good news is that attribution is entirely possible. Law enforcement agencies are increasingly able to track down the bad guys, prosecute them in the court of law, and throw them behind bars. Why is this so?

Firstly, bad guys make mistakes all the time, and these mistakes compromise their Operational Security (OPSEC). This, in turn, enables law enforcement personnel to track and monitor their varied activities closely. Furthermore, they sometimes fall prey to their own greed and inflated egos. Another key point to remember is that a lot of what is happening in cyber-crime has to do with physical world activities like registering a fake company, recruiting money mules, dropping a fake ATM machine on a street corner in New York, and so on.

But much more work is needed to turn the tide against the proliferation of cyber-crime. This takes the form of more focused capacity building for police, prosecutors and judges. And every country has to have a proper legal framework to address challenges in cyber-crime.

In terms of legal framework, I'd like to give you a global view of the different legal instruments that are in place regionally. One could argue that the world today is pretty fragmented in that we have blocks of different countries adopting different regional legal instruments. For example, some countries have adopted the Council of Europe's Convention on Cybercrime, while others abide by the rules of the Shanghai Cooperation Organization (SCO), which is led by Russia and China. One could also argue that in addition to this being a fragmented approach, this represents a differentiated approach to the same problem.

Differentiated by what, you may ask? Well differentiated by ideologies these blocks basically represent as well as competing ideologies on how cyber-space should be run. This is one reason why I believe that it is highly unlikely that we will come to a common legal framework in addressing cyber-crime. One cannot help but wonder what the UN's role in all this would be. Perhaps the UN should be the body that would help to "interoperate and facilitate" between different blocks.

With regard to international instruments that are in place to govern interstate relations, it is often useful to look at how different elements are positioned along a spectrum of conflict intensity. At one end of this spectrum, the Tallinn Manual seeks to provide clarification on the use of force and armed attacks in the cyber context. Up until recently, there was not much clarity on this. I remember a couple years ago I was sitting in the office of the General Manager of a certain agency in the NATO HQ in Brussels, and I asked him whether we could apply NATO Article V in response to a cyber-attack. The key term in Article V is armed attack, so essentially what I was asking is "Could a cyber-operation amount to an armed attack?" Back then the answer was

"no", but we know now the consensus is a cyber-operation is tantamount to an armed attack. There are two main bodies of law that are relevant here: *Jus ad bellum* sets out criteria states must consult before engaging in war, and once states are in an armed conflict, *jus in bello* governs the conduct of war. Article 51 of the UN charter guarantees the right of the state to "use force" when acting in self-defence against an armed attack.

As far as I know, we have not witnessed a cyber-incident that is tantamount to an armed attack; at least not yet. Most of the cyber incidents fall below the threshold of an armed attack. This is where the Law of Countermeasures could be useful. Countermeasures are acts that would otherwise be wrongful acts that the "injured state" takes against the "responsible state" solely for the purpose of compelling the "responsible state" to stop its own wrongful acts. It is important to note that countermeasures cannot be construed as a "use of force", a point we will come back to slightly later. What I'd like to do now is to talk about the implications for states given what we have now.

First, for a state to respond with countermeasure or self-defence, attribution is essential. You have to know who did what to you. If this goes to an international court or tribunal, the burden of proof is on the "injured state" though not to the level of "beyond a reasonable doubt" but it has to be "clear and convincing". Hence, the role of intelligence is really critical here, and given the challenge of technical attribution I think it is important a state combines other sources of intelligence like SIGINT, HUMINT, etc. This applies to anticipatory self-defence as well where a state can only engage in anticipatory self-defence when it is clear on the intention and capability of its adversary. Needless to say, intelligence is all about discovering the adversary's intention and capability.

Now some may argue we could use the "Plea of necessity" to circumvent the issue of attribution because what is important here is not so much of who and what caused this bad situation, but rather what you need to do to mitigate the harm. This has relevance to the active cyber-defence discussion,

but to cut straight to the point, my opinion is if you read Article 25 of the International Law Commission Articles on State Responsibility, you will get a sense that the practical application of the “Plea of necessity” is extremely challenging. You could only use it in truly exceptional circumstances, and one has to demonstrate that the measure taken is the only one available.

Given that attribution can be challenging and time consuming, it makes sense that states possess the ability to take a few hits and continue to function under these degraded conditions. This is why resilience is such an important component of national cyber-power. Let’s go back to the point I made earlier that countermeasures, when taken, cannot be construed as a “use of force”. What that means is if another state knocks out a major portion of your country’s power grid with a cyber-attack, which to me is a clear use of force, and you respond in kind, that is, take out their power grid, it would render the countermeasure unlawful. Hence, the ability of states to combine instruments of national power like diplomatic, economic, politics in their response would be critical to this.

At the end we have to recognise that none of these legal instruments discussed is a panacea for all the problems we will be facing, in fact, there is always a risk that this would end up being a constant “tit for tat” where every state is making the case that it is the victim state and therefore is justified to take action. This increases the possibility of conflict escalation. What is really needed is behavioural norm development and confidence building measures where the focus is on practical measures to mitigate the risk of conflict escalation. Historically, norm development and confidence building measures, especially confidence building measures, have been the work of states. I would argue private sector has an important role to play with this, and here is why.

I have attended a number of cyber policy maker and regulator conferences in the EU, and on a number of occasions there have been suggestions by conference attendees that Cisco could help with influencing countries to

adopt the Council of Europe Cybercrime convention. This underscores the perception that multi nationals like Cisco, which have a global footprint, should have global influence to steer the deliberations toward a certain outcome.

To conclude, one of the things we have to remember is while governments usually own the goal of cyber-stability, they do not necessarily own all the means to shape norms of conduct in the cyberspace. Most of the technical know-how is in the hands of private sector, and it is going to be interesting to see how governments and private sector can come together on this issue.

Networks on Fire: Defending Critical Government Networks

Networks on Fire: Defending Critical Government Networks

Bryce Boland

Many government and commercial networks are now in a state of widespread and persistent compromise. An analysis of 193 compromise assessments in government organisations over a six month period showed 97% were compromised by malware, 75% had command and control traffic leaving their networks, and 31% were compromised by an advanced, persistent threat.

Today's threat actors are nation states, organised criminals and hacktivists. They leverage the Internet to conduct reconnaissance, conduct their attacks and hide their true origins. They target users with dynamic, polymorphic malware via multiple attack vectors.

Cybersecurity has never been more critical. Use of the Internet and other technologies are enabling new operational models that open up governments in vastly different ways, providing citizens with greater speed and access to information but also providing attackers with a perfect platform for conducting cyber-espionage and intelligence gathering.

At the same time the threats are getting more complex, the attackers are becoming more persistent. Attacks have become extremely targeted – in the malware signatures that are seen in our customer's environments, 70% of them are seen only in that organisation, created for that specific attack on that specific target alone.

A new model of cybersecurity is needed to protect against this changing threat landscape.

What is the problem government networks face today?

Every government network is a potential target and possible avenue into critical networks. The challenges for governments include budgets, cybersecurity skills capacity, detection of attacks against critical networks, attribution of threat actors, and ensuring all critical layers are protected adequately.

Despite a focus on cybersecurity, the solution is not free spending on more security controls but finding the right controls. Planning cycles are often long, and funding can come at the expense of more visible initiatives.

Threat actors are using zero day attacks and previously unknown malware. According to a 2013 Ponemon Institute report on *The State of Advanced Persistent Threats*, commercial organisations on average have experienced approximately 9 separate APT-related incidents in the past 12 months. In addition, the report states that 68% of respondents indicate that zero-day attacks are their organisation's greatest threat. These same respondents also overwhelmingly report that advanced cyber-threats have successfully evaded their traditional IDS and AV solutions. These same threat tactics and threat actors also target government agencies.

Protection of critical networks against cyber-warfare requires detection of unknown threats. NATO is considering and developing rules of engagement for defining cyber-war policies, but all government networks need strong defences against the types of zero day and highly advanced threats that are likely to be utilised by state actors against other governments.

Attribution of threat actors is a challenge, as the weaknesses of Internet connected systems make it easy to maintain plausible deniability. Identifying who is attacking may be of high importance in developing an effective response.

Finally, it is a real challenge to protect and secure all critical layers. One layer is not enough in the new threat world. The cost and complexity is high, and defences need to adapt continuously to new attacks.

Risks and repercussions

Today, there are no real risks or repercussions to aggressors from attacks on other nations or theft of intellectual property. The attackers are safe within their own borders, protected by weak law enforcement and judicial capabilities, and widespread weaknesses in Internet connected systems. International agencies have no significant power in many jurisdictions where attacks are routed, making investigation, attribution, and containment of these enemies problematic.

In the past, espionage was expensive, difficult, and extremely risky for the individuals and potentially the countries involved. The advent of the Internet changed all that by dramatically lowering the bar for entry into the world of espionage. Geographic distance, cultural adaption and threat of capture, have all disappeared in cyberspace. This change also creates a low barrier to entry for organised crime and terrorists to also use online capabilities to steal or destroy.

How should governments change their IT acquisition regulations?

According to the Verizon DBIR, there were 1367 confirmed data breaches in 2013. The average number of self-detected intrusions fell from 37% in 2012 to 33% in 2013. Organisations are now less likely than before to detect these intrusions themselves, as the attackers become more sophisticated and stealthy.

The 2013 Mandiant M-Trends report on breach investigations found that

the average time from initial breach to detection is 229 days. One breach went undetected for 6 years. Good enough is no longer good enough. The adversaries have enormous amounts of time to find ways to break in; to defend, requires well-trained teams to identify attacks immediately, prevent them when possible, and mitigate them as quickly as possible when breached to stop data leakage and minimise impact.

You still need good security practices for the basic attacks. But fundamentally, the static defences of the past do not move quickly enough. And that includes the very static IT Acquisition processes with long lead times – a defence against inappropriate acquisitions becomes a means to prolong the static defences.

The reality is that the attacker will map out your static defences, find a pathway to bypass them, and launch their attack. They will bypass your static defences before you deploy them, and moreover, when static defences are active, they will only work against *known* threats.

Most government processes for acquisition are slow, with multiple approvals, approval bodies, review committees, risk reviews, tender processes and so on. Attackers are faster – they don't have to worry about compliance requirements – they just care how they are going to get past whatever defences are in place while maintaining plausible deniability. When defenders change something to catch their latest tactic, they will evolve quickly to evade that.

Acquisition processes need to support the defenders evolving their defences regularly because what works today would not necessarily work tomorrow, and learning from successful attacks needs to happen immediately to prevent the next attack from succeeding.

Governments should work to incorporate security standards into acquisition planning and contract administration. This is a critical step that will enhance the cybersecurity posture of the government. Security standards should

be designed to combat advanced cyber-threats targeting both known and unknown vulnerabilities. These standards should emphasise automated, proactive and dynamic defence by incorporating signature-less, proactive defence.

Recommended attributes of such tools include the ability to:

- Identify and block in-bound zero day attacks across multiple threat vectors;
- Expose the entire attack life cycle by correlating intelligence across various threat vectors;
- Block outreach from a compromised host to its command and control centre;
- Prevent the exfiltration of data and the download of additional malware;
- Eliminate false positives; and
- Produce complete forensic details.

Tools that provide automated sharing of indicators of compromise in near real time should also be included in standard requirements. These enable new threats to be detected more rapidly, and the extent of attack campaigns to be identified.

In addition, governments need ongoing mandatory training and education for contracting officers and other procurement and acquisition officials about evolving cyber-threats with an emphasis on the techniques, tactics and procedures used by sophisticated cyber-adversaries. This will allow them to make informed decisions.

Governments should also support initiatives that enable rapid and flexible acquisition of new cybersecurity capabilities outside of traditional system integration processes.

What baseline standards should be enforced for government networks?

Government baseline standards serve as a role model to incent commercial networks with best practices for cybersecurity. These will improve the posture of the country if critical infrastructure and other key industries are adequately protected.

It is critical to adopt measures that defend against advanced cyber-threats. Incorporating emerging best practices that use behavioural or virtualisation techniques into a security framework and adopting the framework will place governments in a better position to identify and block sophisticated threats.

One example of a best practice that incorporates these approaches into an organisation's defensive posture is the recently released United States NIST Special Publication 800.53 Rev4, Security and Privacy Controls for Federal Information Systems and Organizations, Security Control 44 (SC-44, which defines Detonation Chambers, found in Appendix F-SC, page F-214). In addition to governments, the use of Detonation Chambers as a security control has received widespread adoption across Fortune 500 in the commercial world.

The Australian Signals Directorate (ASD) Strategies to Mitigation Targeted Cyber Intrusions should also be noted in relation to the use of detonation chambers as a best practice for modern defences.

The weakest link

The weakest link is usually human, and this can take the form of ignorance of the threat, and an unwillingness to accept how creative attackers can be. In today's threat environment, every government organisation is a likely target for organised crime, hacktivism and nation-state sponsored spying.

Sophisticated attackers are well organised and will leverage the human and technical weakness, and they will harness any weak government department in order to attack other departments where there is some form of trust or other dependency.

Increasingly, the connectedness of government makes the breach of one department useful for attacking another. Take an example of military defence, the use of air power. Air supremacy depends on planes being able to take off, and knowing accurate weather conditions is essential to battle planning. The network feeds for meteorological information, and the source of that information itself are therefore a significant dependency and communications risk for an air force.

Every department creates some risk for others and the higher the bar across all departments, the stronger the whole will be. Governments need a comprehensive approach to bring agility, situational awareness, and expertise to the protection of all layers of their critical infrastructure, with no department left behind.

India's International Cybersecurity Strategy

India's International Cybersecurity Strategy

Cherian Samuel

India's international cybersecurity strategy flows out of its domestic imperatives and priorities. India has the third largest Internet user base in the world, estimated at around 200 million and poised to grow rapidly with the continued increase in smartphone usage as well as new technologies such as 4G.

As Prime Minister Modi pointed out in his speech at the BRICS Summit in Brazil, India considers cyberspace to be a source of great opportunity but cybersecurity to be an equally great concern. This is not without reason. The government is looking to cyberspace as the main medium to improve and empower the citizen through various e-governance schemes as well as creating feedback mechanisms. Banking, communications and e-tailing are just some of the sectors that have been encouraged to leverage the benefits of cyberspace in providing efficient services.

The threats to the security of cyberspace emanate from various quarters; from hackers to criminals to state sponsored actors. Given the borderless nature of cyberspace, the threats have to be countered through international co-operation. At the same time, capabilities and capacities have to be built up within the country in the areas of law enforcement, forensics and jurisprudence.

The very nature of a borderless cyber-world created by technological and economic innovations is now seen as a construct that questions the very nature of the nation state system. As cyberspace becomes as much a vehicle for transporting ideas and information as it is for transmitting data, much of the heartburn is over the state's lack of control over such a potent medium. This has led to a certain duality of approach in many states, calling for complete control within national territories while endorsing the idea of cyberspace being subject to minimal control internationally.

While not as engaged with the intricacies of cybersecurity and Internet governance as it should be, India has viewed cyberspace as a global commons “which no one state may own or control, and which is central to life as we know it today”. This hands off approach is no longer tenable, in part because of the reality that cyberspace requires some governance and regulation. Many states that previously championed this perspective now sing a different tune. The United States, for instance, now contends that while cyberspace might superficially resemble other global commons like air, sea and space, the physical infrastructure was the property of different entities making such comparisons moot. In the speech referred to above, the Prime Minister described cyberspace as a global public good, which would logically necessitate some discussion and negotiation on mutually agreeable norms and practices.

India has held the position that such discussions should follow the principles laid down in the Tunis Agenda, which gives primacy of position to governments when it comes to resolving issues that are primarily in their domain. The Agenda was prescient in noting that “Policy authority for Internet-related public policy issues is the sovereign right of States”, and that “they have rights and responsibilities for international Internet-related public policy issues”. With most Internet-related public policy issues increasingly impinging on the sovereign right of states, a suitable mechanism and framework needs to be drawn up to ensure the continuance of cyberspace as a domain that is open, global and secure. It is to this end that India proposed a Committee for Internet-Related Policies (CIRP) to the United Nations in 2011. This would be a more permanent form of the UN Group of Governmental Experts (UN GGE) that has had three iterations so far and presented two reports.

While the UN GGE has done sterling work in laying out a roadmap from Cyber Confidence Building Measures (CBMs) to norm making, its cyclical nature and the turnover in members constrain its abilities to perform a more durable role. It has also outsourced the work of implementation to sub-regional organisations that have varying degrees of expertise and capacity. In Asia,

the two main multi lateral organisations dealing with cyber security are the OIC-CERT and APCERT with a certain amount of overlap in membership. Organisations like APCERT need to be more pro-active, going beyond the two table-top exercises held a year to more intensive capacity-building programs. The ASEAN Regional Forum (ARF) has also initiated a cyber security program designed to bring together experts from governments, international organisations, academia, and the private sector. On the whole, there is a need for a more dedicated mechanism for co-operation that covers the whole of Asia, and is Asian-led. The lack of co-operation and dialogue within the region is exemplified by the fact that India has bi-lateral cybersecurity dialogues with more countries outside the region than within.

At the bi-lateral level, India has cybersecurity dialogues with other major cyber-powers, including Japan, South Korea, the United Kingdom, France and the United States as well as the European Union. Outcomes have been in the form of training programmes, intelligence cooperation and research and development funding for joint projects. The nodal agency for securing cyberspace, CERT-In has signed agreements with overseas CERTs such as USCERT and Korean Internet Security Agency (KISA).

In the short term, India's cybersecurity goals include building up capacities at home to provide a safe and secure cyberspace, and forging co-operative relationships internationally – bilateral as well as multi-lateral as part of that goal. Issues that have to be tackled over the long term include the re-structuring of Internet governance to better reflect the requirements of the times and the establishment of norms and conventions to moderate the excesses by way of cyber-intrusions, which, if left unchecked, could have unforeseen consequences.

Enhancing ASEAN-wide Cybersecurity: Time for a Hub of Excellence?

Enhancing ASEAN-wide Cybersecurity: Time for a Hub of Excellence?

Caitríona H. Heinl

The ASEAN ICT Masterplan 2015 (AIM2015) envisions creating a global Information and Communications Technology (ICT) hub. The grouping's ambition is to distinguish itself as a region of high quality ICT infrastructure, skilled manpower and technological innovation. In support of these plans, member states should spur the creation of a cybersecurity hub of excellence in the region as part of a wider comprehensive cybersecurity strategy.

Lack of region-wide cohesiveness

National and regional moves to adopt comprehensive cybersecurity strategies have been somewhat slow and fragmented across the globe. To date, ASEAN's efforts to adopt a comprehensive regional framework for cybersecurity are equally piecemeal.

This lack of region-wide cohesiveness does not help the region's security and impairs the ASEAN Economic Community Blueprint to become a single market and production base, a highly competitive economic region, and one that is fully integrated into the global economy. Indeed, an ASEAN-wide comprehensive cybersecurity framework has yet to be developed, official public documents are vague, the 2014 schedule for ASEAN official meetings does not include cybersecurity, and the precise extent of discussions and proposed initiatives is difficult to ascertain.

Creating a Regional hub of Cybersecurity Professionals

Congruent with ASEAN's aims to develop a workforce with high-level ICT

proficiency, member states should develop a pool of cybersecurity professionals to effectively respond to regional and international cybersecurity challenges. This could be achieved through a range of approaches and programmes including ASEAN cybersecurity scholarships (like those proposed under the Mactan Cebu Declaration and AIM2015 for an ASEAN ICT Scholarship programme to attract ICT talent); education on cybersecurity issues at the earliest possible age as well as incorporation in school curricula; the further development of "ASEAN Cyberkids Camp"; and initiatives to encourage and attract talent to choose ICT as a career.

Innovative initiatives like CoderDojo could also be considered by ASEAN member states as a novel way to attract young talent for the purposes of regional cybersecurity. CoderDojo is a cost effective and largely community-driven global movement sweeping across Europe and the United States with more than 15,000 children learning to write software in more than 35 countries. Currently, there is one CoderDojo in the ASEAN region (CoderDojo Bandung, Indonesia), five in India and eight in Japan. It runs free not-for-profit coding clubs in local communities and regular sessions for young people to learn how to code and develop websites, apps, and programs in a fun environment.

In China for instance, one out of three school children already want to be a "hacker" when they grow up – hackers are the new cool, the new rock star. To attract such young talent, "Dojos" also organise tours of technology companies and introduce guest speakers to talk about their careers. Its focus on young girls and women in technology at DojoCon2013 in April this year is particularly noteworthy for the ASEAN region.

ICT experts and innovators

AIM2015 calls for the establishment of a database of ICT experts and innovators within ASEAN, which could be harnessed for cybersecurity professionals. Furthermore, accrediting IT and cybersecurity professionals

with a regionally-recognised certification should also be considered to allow for regional cohesiveness. As it stands, ASEAN has completed eight Mutual Recognition Arrangements (MRAs) to facilitate the free movement of skilled labour in the region, albeit to varying degrees of cooperation in recognition of qualifications. However, of the eight professional groups listed, computer scientists and IT professionals are not listed (although engineering services are included).

It is also worth considering the European Commission's recent proposal under the February 2013 Cybersecurity Strategy of the European Union of a roadmap for a "Network and Information Security Driving Licence". If implemented, this would be a voluntary certification programme to promote enhanced skills and competence of IT professionals. Furthermore, the Commission plans to organise with the support of the European Network and Information Security Agency (ENISA) in 2014, a "cybersecurity championship" where university students across the region will compete in proposing network and information security solutions.

Finally, to stimulate a culture of security and data privacy by design, the Commission recommends the introduction of training on network and information security, secure software development, and personal data protection for computer science students.

Fostering a "win-win solution"

Such measures will further increase the attractiveness of ASEAN for foreign direct investment and enhance the region's competitiveness. ICT is regarded as a growth sector for the region, employing nearly 12 million people and contributing more than USD32 billion to ASEAN's GDP, with figures expected to increase by 2015.

These initiatives will also address the development divide, help alleviate

poverty, and create employment opportunities in line with the social development goals of the ASEAN Community and the Millennium Development Goals of the United Nations.

While there is no one-size-fits-all approach for this developing area, it is in the common interests of ASEAN states – and the wider international community - to adopt such regional initiatives for cybersecurity to tackle cross-border cyber threats. The current lack of region-wide cohesiveness and a comprehensive framework is detrimental not just to the realisation of the ASEAN Economic Community but also to the overall security of the ASEAN region.

Significantly, it will also impede current and future international cooperation efforts on cybersecurity that are required to deal effectively with the cross-border nature of cyber incidents.

*Originally published as RSIS Commentaries, No. 133/2013 dated 18 July 2013

Enhancing Cybersecurity: Improving Technical and Analytical Expertise in Singapore

Enhancing Cybersecurity: Improving Technical and Analytical Expertise in Singapore

Damien D. Cheong

A 2013 *Straits Times* report highlighted that Singapore, like many other countries such as the United States, United Kingdom and India, was experiencing a shortfall in the number of cybersecurity practitioners. Furthermore, graduates did not seem attracted to the IT security profession, which meant that the next generation of cybersecurity practitioners would be negatively impacted.

Expectedly, these trends are a cause for concern in light of the persistent and ever-increasing cyber threats facing the country. The government has embarked upon two major initiatives to address these issues.

Role of strategic analysis

Firstly, it has increased the number of scholarships for infocom security studies through the Infocom Development Authority (IDA). Secondly, it has announced two different training initiatives for potential and existing cybersecurity practitioners: (a) KPMG's Cyber Security Centre in collaboration with Singapore Polytechnic will conduct cybersecurity courses for 10 to 15 participants annually; (b) FireEye, a security company specialising in advanced cyber threat detection, will train existing cybersecurity practitioners to hone their skills in detection analytics, identification and monitoring of emerging threats as well as undertaking "defensive action".

These initiatives are both timely and necessary. In addition, they will need to be complemented with a corresponding increase in strategic analytical training. This is envisaged to significantly improve the quality of analytical products as better strategic insights can be generated.

The major challenge of data analysis in the “era of Big Data” is well-known; it is both time-consuming and involves a lot of manpower to make sense of it all. Even if technological advancements help minimise the time taken to filter useful data from non-useful data, the resultant data still lacks strategic insights. As a result, the value of the analytical product to decision-makers is somewhat reduced.

Enter the strategic analyst. His/her job, effectively, is to analyse data and convert it into useful information. This, according to Thomas Fingar, former chairman of the National Intelligence Council, is accomplished by “providing insight on trends”. Such insight adds value to the information, and allows the decision-maker to “broaden the range of possible futures and thus better manage uncertainty”. Hence, effective data collection and functional analysis, while a major part of cybersecurity expertise, must be buttressed with “strategic analysis of threats and threat indicators”.

Strategic analysis, according to the Software Engineering Institute (SEI) at the Carnegie Mellon University, “adds perspective, context, and depth to functional analysis, and incorporates modus operandi and trends to provide the ‘who’ and ‘why’ of cyber threats. It is ultimately rooted in technical data, but incorporates information outside traditional technical feeds – including internal resources such as physical security, business intelligence, and insider threat, and external feeds covering global cyber threat trends, geopolitical issues, and social networking.

The resulting strategic analysis can populate threat actor profiles, provide global situational awareness, and inform stakeholders of the strategic implications cyber threats pose to organisations, industries, economies, and countries.

Improving strategic analytical capabilities

Researchers at the SEI have proposed several measures to improve strategic analytical capabilities in their report Intelligence Analysis for Internet Security. These include:

Overall Threat Assessments: Pertains to the "analysis of vulnerabilities of critical missions (including levels of dependence), the kind of disruption and damage that could be caused to the implementation of these missions, the kinds of weapons/instruments that could be used to cause such disruptions and the likelihood of such attacks and intrusions taking place".

Sector Threat Assessments: Focuses on "vulnerabilities and threats either in particular areas such as national infrastructure, or in particular sectors of the economy such as banking or e-commerce…In effect, a strategic analysis of this kind has to take account of changes in what can be a very dynamic environment".

Trend Analysis: Relates to analysing "changing threats and vulnerabilities. These might include base-line assessments so as to better recognise departures from the baseline. Alternatively, they might focus on future threats and vulnerabilities in an effort to determine in what ways the problem is evolving – and what can be done to anticipate and contain future challenges. Trend analysis is likely to be most effective when it is linked with careful attention to drivers such as key trends in the political, economic, social and technological sectors that will shape the future threat and vulnerability environment of the future.

Potential Damage Assessments: Assesses the "potential cascade effects of intrusions. This would offer opportunities to develop both defensive and mitigation strategies. Crisis management, contingency planning, mitigation strategies, and disaster management would all be enhanced by strategic analysis of potential damage assessment. Indeed, the capacity for effective and rapid reconstitution might depend on such analysis".

Categorising and Differentiating Attacks and Attackers: Differentiating between intrusions/threats from various sources is critical. “This will be especially true as groups or individuals develop intrusion strategies that mimic other forms and thereby lessen their chances of identification or, in the case of nation states, provide plausible deniability of their actions. Also, by doing so, appropriate responses that might go beyond simply defensive or mitigation strategies can be determined”.

Identification of Anomalies: This refers to detecting “anomalies that provide indicators of emerging threats and problems”. Anomalies in this context can be understood as developments or events that do not fit typical or known patterns. The detection of anomalies or novel patterns can be a major element in anticipating new methods of intrusion, new targets, or even new classes of intruders. “It is a macro-level task that requires careful and systematic ‘environmental scanning’ as well as the coalescing of tactical and operational intelligence reports that identify and highlight specific aberrations from the norm”.

Analysis of Future Net Environments: This provides “assessments of potential future environments on the Internet and the potential impact of malicious activity within those environments”.

Some of these measures will most likely be taught in the new IT security courses. Nevertheless, it may be useful for public as well as private organisations to audit current capabilities to determine if their strategic analytical expertise requires enhancement. In light of the inadequate regulatory/legal frameworks at the international level to deal with cyber threats, defence, through improving a country’s cybersecurity capabilities, is the best approach to cyber-threats at present.

*Originally published as RSIS Commentaries, No. 024/2014 dated 5 February 2014

Securing Cyberspace: Whose Responsibility?

Securing Cyberspace: Whose Responsibility?

Senol (Shen) Yilmaz and Kah-Kin Ho

The defacements of websites of governments and businesses are a great nuisance to the victims. However, Anonymous, the network of hackers behind these defacements, declared its intention to create more than just nuisance. In a video published in 2013, the network threatened to attack the financial sector of Singapore to “cause financial loss”. It remains to be seen whether Anonymous is able to carry out cyber-attacks that would result in significant financial damage.

The fact, however, is that critical infrastructure – whether in the finance, transport, energy, or utilities sector – is highly vulnerable. In 2012 for example, the so-called Shamoon virus caused severe disruptions by wiping out data from thousands of computers at Saudi Aramco, the largest oil producer in the world. Allegedly carried out by Iran, a state-actor, it took the company two weeks to recover from the attack.

Critical infrastructure vulnerabilities

It has been demonstrated that when critical infrastructure is attacked severe disruptions can follow. Further aggravating this situation is that more and more machines connect to cyberspace and become remotely controlled. These include control systems of gas and oil pipelines. In the not too distant future, even more devices will be interconnected ranging from those critical for national security as well as household goods and cars. When targeted jointly in a mass attack, even private consumer goods could turn into a national security threat.

Given the likely increase in vulnerabilities governments worldwide agonise over the right approach to making cyberspace more secure.

From governments' point of view, protecting critical infrastructure poses two difficulties. First, in many countries, the operation of critical infrastructure as well as the physical and intangible components of cyberspace is held in private hands. Due to private ownership, governments often do not exercise immediate operational control. Even standard-setting for the Internet is not always carried out by national governments, or inter-governmental bodies, but in open standards organisations such as the Internet Engineering Task Force, where governments have limited say.

Second, governments and the private sector have divergent interests: Governments on the one hand are concerned with ensuring national security while maintaining or creating an environment conducive for economic activity.

The private sector on the other hand has as its main objective making profits and serving shareholder interests. In terms of security, it does what it deems "enough" which may not necessarily be sufficient. In general, every extra dollar spent on security decreases corporate efficiency and shareholder value in the short-term. Incentives to invest in additional security measures are often only recognised once perpetrators have successfully compromised systems. This can be too late in the case of a serious cyber-attack that may cause substantial damage.

Government lead or private sector starring?

In the context of assigning roles, two diametrically opposing views have emerged. The first argues that corporations have made huge efficiency gains through the computerisation of operations. For example, banks can operate their business more efficiently by allowing their customers to make e-transactions from their homes without interacting with a clerk. Similarly, utilities providers no longer send staff to manually activate valves or switches located far from central operation sites.

Rather, the same operation is commanded remotely from a machine, with minimal human action. For these reasons it is argued that the private sector should not only reap the efficiency gains of such automation and computerisation but also share the burden of hardening the infrastructure on which they depend.

The opposing view puts forward that securing the nation is one of the most fundamental tasks of governments. Nobody would expect the operator of a hydroelectric power station to protect its dams against ballistic missiles from adversaries. It is argued that no other standard should apply to figurative cyber-missiles that could result in similar damage.

Framework for PPP: collaborate, facilitate, regulate

Arguably, it would be reasonable to share the burden of protecting cyberspace in public-private partnership (PPP). However, there is no magic formula for assigning the roles that governments and the private sector should assume. The culture of governance differs substantially between countries ranging from very little public sector involvement to heavy regulation. Nonetheless, a three-pronged framework could help in this endeavour: there is need for collaboration, facilitation and regulation.

First of all, close collaboration at all levels is crucial. Exchange of information and best practices, or collaboration in screening and analysing malicious Internet traffic between Internet Service Providers and governments' Computer Emergency Response Teams (CERTs) can reduce cyber-threats.

Secondly, governments can facilitate the implementation of cybersecurity measures by providing reliable guidelines and by creating the right incentives. Investments in additional measures could be awarded tax breaks and low interest loans could be provided to companies that invest in the resilience of their systems. Furthermore, governments could consider cybersecurity measures that are in place when granting contracts to businesses.

Last but certainly not least, cybersecurity will likely not be achieved without any regulation at all. Obviously, corporations tend to loath being regulated since regulation can be burdensome and inhibit profit-making. However, governments can develop regulation in close cooperation with the private sector. Richard Clarke, former Special Adviser to the US President for Cybersecurity, suggests “smart regulation” is also possible: regulatory end-goals are defined but the best avenues to reach such goals are co-developed with the private sector.

Equally important, legislative processes need to be accelerated to provide timely guidance to narrow the gap between ill-boding technological advances and regulation. The faster governments react, the less the chance of damage.

Admittedly it is a difficult task to balance the interests of governments and the private sector. However, close public-private partnership can prevent mere cyber-nuisance from transforming into a national security threat and finally lead to a win-win situation: an environment conducive for economic activity in a secure nation.

*Originally published as RSIS Commentaries, No. 210/2013 dated 12 November 2013

Effective Public-Private Cooperation for successful Cyber-crime Investigations – Capacity Building against Cyber-crime

Effective Public-Private Cooperation for successful Cyber-crime Investigations – Capacity Building against Cyber-crime

Cormac Callanan

My focus is different from many of the other experts, and is on the narrow subject of cyber-crime. This area of interest describes the practical challenges of real crime using the Internet or exclusively on the Internet which affects real citizens across the world. It deals with groups of identifiable criminals, often operating in organised groups, who exploit computer and network vulnerabilities to commit crime against our friends, family and neighbours who have minimum knowledge and expertise to mount a coherent defence.

Many of the other experts clearly demonstrate expertise and knowledge in the area of cyber-warfare and cybersecurity. There has been a significant body of research which has been undertaken by all these experts over the last few years with specific focus on what constitutes an act of cyber-warfare, when would a state be reasonably and legally authorised to respond to acts of cyber-provocations and what rules of engagement would cover any response.

I have an industry background and I have spent the last decades of my career working in the area of cyber-crime. Initially, this was in the area of combating child pornography in the International Network of Internet Hotlines (INHOPE). More recently this was as Industry Coordination in 2CENTRE, the Cybercrime Centres of Excellence Network for Training, Research and Education, encouraging close collaboration between academia, law enforcement and industry in cyber-crime investigations. I have worked as a cyber-crime expert for the European Commission, the Council of Europe, the Organization for Security & Cooperation in Europe and the United Nations Office for Drugs & Crime in Vienna.

I understand and appreciate the need for states to focus on the development of agreed international protocols as they relate to acts of cyber-warfare and attacks against states. We need methods and agreed protocols to reduce tensions and to de-escalate cyber-conflicts. Nonetheless, cyber-crime is happening around us daily and cyber-crime investigations are a huge challenge for law enforcement, prosecutors and judges today.

The Internet is global, has no borders and is changing, adapting and evolving. Governments and national law enforcement are challenged by the transnational dimension of the Internet. At the same time, harmful and illegal content and activities on the Internet cross national borders and directly affect citizens.

In Europe, the European Cybercrime Centre (EC3) based in Europol in The Hague is the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. EC3 commenced its activities on 1 January 2013 with a mandate to tackle cybercrime with specific focus on crime committed by organised groups to generate large criminal profits such as online fraud, crime which causes serious harm to the victim such as online child sexual exploitation and crime which affects critical infrastructure and information systems in the European Union.

A typical online crime can span a wide range of countries with a long list of participants in the criminal chain, each with limited knowledge of upstream and downstream participants and most often the perpetrator(s) are not located in the same countries of the victims. Indeed a complex network of international connections can be created and maintained through a range of third countries by the criminal enterprise with minimum cost and technical knowledge. In some cases computers owned by innocent victims are used in the criminal plot to attack other victims or host illegal content.

The range of illegal activities on the Internet continues to evolve. Unsolicited email (SPAM) causes significant impact on network efficiencies with large

volumes of bandwidth, email servers and staff time being taken up in managing and restricting such communications. Many of the skills learned in this area are then applied to other areas of concern such as child abuse and intellectual property violations. Child Sexual Abuse Material (CSAM) continues to grow as Internet usage continues to grow. Malware also causes significant impact on end users with new major concerns in mobile space and increased impact on desktop based systems. Many countries are concerned by the impact of online gambling and the loss of exchequer revenues if taxes related to online gambling are lost. A separate area of huge growth is that of online drugs including illegal drugs, prescription drugs (available on the Internet without prescription) or fake drugs which can be damaging. Online crime continues to evolve and recently we have witnessed an increase in attacks in mobile devices and on online extortion through ransomware.

Trans-national cyber-crime investigations are challenging, and there is a need for national law enforcement agencies to work closely with each other internationally in order to successfully prosecute online crime. Few law enforcement agencies are actively funded or are encouraged to cooperate with foreign agencies, and a range of barriers need to be surmounted.

Appropriate legislation is a major concern. There are few international instruments on the legal definitions of cyber-crime and procedural instruments are equally effective and it is important to ensure that national legislation is comparable internationally. One of the earliest international instruments is the Council of Europe Cybercrime Convention, which was created in 2001 and many regional and national instruments have been created since.

However, responding to the challenge of cyber-crime is not exclusively a role for law enforcement. Since 1999 an international NGO called INHOPE, the international network of Internet hotlines has worked to protect children and remove online child abuse material from the Internet and simultaneously empower faster investigations by law enforcement. In 2013, the INHOPE network consisted of 49 Internet hotlines in 43 countries where 170 analysts

processed 1,210,893 reports of illegal content and 54,969 reports were assessed to contain unique URLs of child sexual abuse material. One example of swift international collaboration enabled by the network occurred in June 2013 when the Irish Hotline.ie had a major success in cooperation with INHOPE colleagues at Taiwan's Web547 hotline. Hotline.ie received an anonymous report about a forum posting involving 520 child sexual abuse material (CSAM) videos. Hotline.ie traced the videos to Taiwan and forwarded the details to the Web547 hotline. Their analysts uncovered a further 408 locations on this service containing more CSAM. In all, 908 video and picture archives were reported to law enforcement agencies and the relevant Internet service provider, resulting in the rapid removal of the illegal material from the Internet.

Cyber-crime investigations today are further challenged by the increase in the workload of cyber-crime investigation units, the increased complexity of the cases which are being handled, the reduced resources available in the current global economically-challenged climate and the high expectations from citizens and the judiciary in the quality, efficiency and effectiveness of the criminal investigation.

Investigators have insufficient training options in IT forensics and cyber-crime investigations, and in Europe, generally rely on courses provided by Europol and/or Interpol. A number of countries have developed their own law enforcement cyber-crime training programmes either alone or in conjunction with academic institutes. Law enforcement has also availed of a large number of training courses, seminars, conferences and hands-on training provided by different industry players in locations throughout the world. These methods are not scalable or sustainable and do not follow a training path or provide a standard assessment of knowledge or competence. Therefore, it is difficult to measure the usefulness and effectiveness of these efforts. Current international cross-coordination of training activities is limited and relies on a few individuals to drive the activities. The 2Centre network was created in order to provide academically accredited training in a modular format

developed in cooperation with law enforcement and industry targeted at the cyber-crime forensics investigator. These centres of excellence collaborate in a network to ensure minimum duplication of effort, high quality training and research, shared with others in the network to ensure consistency and scalability compatible with cultural and linguistic sensitivity.

One of the greatest challenges on the Internet today is increasing user confidence and security, which is hampered by large scale highly visible malware attacks. As far back as 2009, the Australian Cyber Security Report highlighted concerns in these areas when they said that “Australia’s national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies ICT”. This view would be common among many countries of the world. The report went on to state that “the production, sale and distribution of malicious code has become a prolific criminal industry, making malware stealthier, more targeted, multi-faceted and harder to analyse and defeat”. This is further compounded by the fact that the report also confirmed that “there is a growing array of state and non-state actors who are compromising, stealing, changing or destroying information and therefore potentially causing critical disruptions to Australian systems. The distinction between traditional threat actors – hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services – is increasingly blurred”.

It is not clear the level of determination or resources that will be available to an adversary. Some of these adversaries might be state actors. The disclosures by Edward Snowden, former NSA consultant, have dramatically increased concerns by users and even states around the world about Internet security, confidentiality and privacy. The software programming vulnerabilities uncovered in the Secure Sockets Layer have further increased uncertainty.

As a result of these disclosures, the issues surrounding national security is broadly discussed in society today, and it is clear that the widespread

collection of data on the Internet – both private and open-source intelligence – provide higher levels of profiling and tracking than ever before. Large volumes of traffic, subscriber and billing data is often stored by Internet industry stakeholders and disclosed to authorised state agencies based on democratic laws adopted by national parliaments. These same parliaments provide oversight that such systems function properly.

It is important to differentiate between data retention and data profiling conducted by national security in different countries and the activities required for the investigation and prosecution of criminal acts. In areas indicated before, such as online child abuse or attacks against computer systems, there is an ongoing need for access to data records in order to investigate online crimes, identify offenders by gathering evidence and for the exoneration of innocent third parties.

Many reasonable and proportionate strategies have been painstakingly developed over the last decade for effective cooperation between the Internet industry and law enforcement to support criminal investigations. It would be a great pity if they were disbanded or disrupted as a result of widespread fears and concerns about overreaching national security agencies across the world.

Applying Insights Gained from Traditional TCBMs to Cyberspace

Applying Insights Gained from Traditional TCBMs to Cyberspace

Ulrich Kühn

The key objectives of classical Transparency and Confidence-Building Measures (TCBMs) are: stability, trust-building, predictability, reciprocity, transparency and reliability. Traditional TCBMs are an inherent part of the policies of cooperative security in Europe under the auspices of the Organization for Security and Co-operation in Europe (OSCE). During the last 40 years these policies have undergone a number of fundamental shifts and changes. This period has seen the tentative emergence of the paradigm of cooperative security, including early TCBMs between the two blocks during the 1970s, the establishment of a number of legally and politically binding TCBM and arms control regimes during the late 1980s and early 1990s, the adaptation of these instruments during the mid and late 1990s, eight years of stagnation and regression from 2000 to 2008, attempts to reset and repair the regime complex between 2009 and 2011, and the slowdown of policies, followed by the current Ukraine conflict. A number of important insights can be gained from the history of the establishment, maintenance and decay of the TCBMs.

The scope of traditional TCBMs in the European context falls into several categories. At the level of principles and norms, the early TCBMs stress: strengthening of peace and security, strengthening of confidence, increasing stability, the territorial integrity of States, sovereign equality, the complementary nature of the political and military aspects of security, the indivisibility of security, reciprocity, reducing the dangers of armed conflict, promoting disarmament, promoting military exchanges and the further development of these measures. Their main scope can be subsumed under the headline of establishing a continuous dialogue to reduce the risk of conflict. Not surprisingly, these principles and norms are rather vague, sometimes contradictory, and often articulated as principles of the lowest common denominator.

With respect to the working agenda, the European experience produced a number of politically binding TCBMs, such as the Stockholm Document of 1986, the Vienna Document (VD) of 1990 (which was updated in 1992, 1994, 1999, and 2011) and the Program for Immediate Action Series, which resulted in eight documents with various scopes, such as: (a) a Program of Military Contacts and Cooperation; (b) Stabilising Measures for Localised Crisis Situations; (c) Principles Governing Conventional Arms Transfers; (d) Defence Planning; (e) a Global Exchange of Military Information; (f) a Code of Conduct on Politico-Military Aspects of Security; and (g) specific Principles Governing Non-Proliferation. These documents are all of a politically binding nature. They are all operational, some of them are outdated, and some of them are porous. However, they still have their value, even in today's security environment.

A good example is the Vienna Document (VD). The VD's provisions are manifold, and can be subsumed under the categories of information exchange, communication, notification, and verification. In the current Ukraine conflict, the VD has been implemented to gather information about the Russian forces close to the Ukrainian border. However, Russia has used loop holes in the VD by, for instance, splitting up forces involved in manoeuvres so that they did not fall under the VD's thresholds for notification.

In the dimension of legally binding measures, the Treaty on Conventional Armed Forces in Europe (CFE), established in 1990, limits the number and movement of certain types of heavy conventional weaponry. The CFE Treaty is both a disarmament as well as an arms control treaty with strong TCBM features. Its provisions contain notifications and on-site inspections. This treaty is accompanied by the Treaty on Open Skies, a legally binding instrument to monitor compliance with CFE. Following the adaptation of CFE, to take into account NATO's eastward enlargement, the treaty came under intense pressure. Due to political disputes between NATO and Russia pertaining to Russian forces in Georgia and Moldova, the treaty collapsed in 2007 and efforts to revive the agreement have failed ever since.

From this short overview, a number of insights can be gained. First, in terms of institutionalisation, the establishment and maintenance of security regimes and their successful adaptation and transformation into regime complexes neither inevitably leads to a state of eternal stability nor to the emergence of a security community, where the threat of war is absent. Rather, such processes can be volatile, sometimes dysfunctional, and can erode over time if the actors fail to agree on timely measures, which promise equivalent gains for the most important players.

Second, the establishment of dialogue mechanisms is often the first tentative form of an actual TCBM. It is argued that the more inclusive the framework, the higher the chance of it being a continuous endeavour. And the more open the formulations, with respect to principles and norms, the easier it is to agree on a working agenda. However, established and once agreed-upon principles and norms are hard to change over time.

Third, the extension and continuation of TCBMs over several years are often accompanied by learning effects. This form of actors' cognitive repercussions for the actors, which makes continued implementation, even in times of crisis, more likely. However, TCBMs have no built-in 'compliance guarantee'. Further on, they are not likely to prevent a crisis from escalating if actors have a mutual interest in escalation. Nevertheless, they do provide important consultation mechanisms when other channels of communication are blocked.

Fourth, even legally binding accords, such as the CFE, can erode over time if the interests of major actors are divergent. Particularly efforts at "social engineering", such as the adaption of existing institutions, can result in the weakening of instruments. If not carefully handled, it can even contribute to their erosion.

Potential applicability of TCMS to cyberspace?

Are traditional TCBMs applicable to cyberspace? In comparison with the field of traditional military confidence building, cyberspace suffers from a lack of definition, as well as a puzzling diversity of actors, assets, areas, and accountability. In the traditional military realm, actors are states and their national forces. In cyberspace, actors are states, their national forces, and intelligence services, as well as NGOs, private businesses of all sorts, specific peer groups, and the individual human being. A clear distinction with regard to attribution, for instance, in the case of a cyber-attack, is almost impossible if such an attack is carried out in a sophisticated manner. As a result, TCBMs for certain actors, such as specific transparency measures on air force capabilities, are hard to apply in cyberspace, particularly since states are hesitant to reveal if and which state-driven actors are part of a military cyber command.

Except for man power, traditional military assets are weapons and related military equipment. In cyberspace, almost all assets (hardware as well as software) are of a dual-use character, that is, they could be used for cyber-attacks as well as cyber-defence. They can be militarily applicable or designed for purely civilian purposes. Furthermore, they are cheaper and easy to obtain. A clear distinction about which assets are purely military is therefore impossible. As a result, potential transparency and particularly verification measures as well as possible cyber-TCBMs in the realm of asset non-proliferation are very hard to pursue. This would require an extremely high degree of cooperation and transparency willingness amongst a multitude of actors.

Areas are defined by geography and national borders. Traditional TCBMs and limitations normally apply to specific geographic areas of heightened tensions in, for instance, border regions. None of these exist in cyberspace. Possible transparency or even limitation measures in cyberspace would need a totally new definition of areas, most likely not with respect to national

space, but rather with a view to critical key installations, such as underwater cables, server knots, crucial power grids, nuclear installations, stock markets, or even larger hospitals.

In the traditional military realm, accountability lies with the nation state as well as with international organisations (particularly in the realm of verification of compliance with TCBMs). In cyberspace, however, accountability again lies with a multitude of actors (most of them non-military). Distinguishing lines are additionally blurred by the relatively cheap technical ability to disguise particular actions. Furthermore, international cyber-policies demonstrate a critical lack of governance, which triggers a lack of commonly agreed principles and norms – the basis for any future cyber-TCBMs.

As a consequence, most traditional forms of military TCBMs are either non-applicable to cyberspace or would encounter serious obstacles. Nevertheless, an initial set of cyber TCBMs, under the auspices of the OSCE, has been developed in recent years. Consensus among the 57 OSCE participating States is a success per se, and represents the most advanced effort so far.

Given the unique character of cyberspace and the associated technical obstacles, lessons learnt from the European TCBM experience are more likely to be found in the evolution and maintenance of a political process of cooperation than in specific provisions from the traditional military realm. Therefore, the next steps will be crucial for maintaining this fragile process.

To begin with, states will have to make a concerted effort to formulate a set of common principles and norms relating to cyberspace and cybersecurity. This suggests that states will have to make an effort to broaden the dialogue with other actors. Any future dialogue should be inclusive with respect to national actors (of which the United Nations may be the appropriate forum), and involve commercial as well as private actors. As this will represent a completely new political endeavour, new options to broaden the discussion, such as working seminars on national cyber-doctrines, the establishment

of joint risk reduction centres for data exchange, or mixed national-civil capacity-building efforts will be needed. Such a multi-level dialogue would be a TCBM itself.

Furthermore, before the establishment of any principles and norms, actors will have to work on commonly agreed definitions of disputed terminology, such as cyberspace, strategic cyber-warfare, cyber-attack, or cyber-sabotage, to mention just a few.

Finally, any common principles and norms will have to be crafted cautiously in order to bridge huge normative gaps.

As European history has shown, even close geographic proximity does not automatically trigger a common normative understanding. With regards to the different global regions, divergent norms and values will have to be taken into account. Pursuing concrete TCBMs which go beyond regional aspects might be easier, once a certain normative foundation which addresses normative divergence and normative convergence has been worked upon.

US-Russian Confidence Building Measures in Cyberspace: Historical Background and Perspectives

US-Russian Confidence Building Measures in Cyberspace: Historical Background and Perspectives

Oleg Demidov

The track record of the US-Russian bilateral cooperation on the issues of ICT and cybersecurity in a global security context probably dates back to the end of the 1990s when this agenda, for the first time, emerged in bilateral negotiations. One major step at that early stage of the bilateral dialogue was the meeting of the US and Russian Presidents and the resulting Joint Statement "The Common Security Challenges at the Threshold of the 21st Century" signed on September 2, 1998. The first document of its kind, the Statement addressed the ICT related issues in the context of international security, and raised several important points such as "…promoting the positive aspects and mitigating the negative aspects of the IT revolution", "ensuring the future strategic security interests" of the US and Russia, including the ICT agenda; and "resolving the potential Year 2000 computer problem". The Statement also called for the launch of bilateral consultations and study of the wider consequences of potential common challenges, including those in the field of the ICT.

This episode, which clearly marked the start of US-Russian bilateral dialogue on ICT issues in the global security context, did not receive a consistent logical development in the immediate term. It took some time before the issue of ICT in the security and military context was included in the framework of US-Russian bilateral negotiations. After more than a decade, things have now changed.

In February 2011, a call for a high-level cybersecurity bilateral working group originated from Moscow. And in June 2011, the meeting of the US and Russian delegations took place in Washington, DC, with the aim "to continue discussions of confidence-building measures, with the

goal of preventing misunderstanding and inadvertent escalation of cybersecurity incidents".

After a few days of negotiations, a Joint Statement was adopted by the USG Cybersecurity Coordinator, Howard Schmidt and the Deputy Secretary of Russian Security Council, Nikolai Klimashin. The Statement laid the basis for all subsequent bilateral negotiations and discussions in this area; it also very clearly reflected the changes that the information security (or ICT security) agenda had undergone since 1998 (It had become much more concrete, diversified and truly strategic). The negotiations of the two delegations and the Statement itself were focused on three main issues:

1) The exchange of military views on cyberspace operations
2) Implementation of regular information exchange between both nations' Cyber Emergency Response Teams (CERTs)
3) Establishment of protocols to communicate about cybersecurity issues via existing risk reduction/crisis prevention communications links between Moscow and Washington

Further steps were required after the new start. The Joint Statement of June 23, 2011 called for implementation of the steps of practical bilateral cooperation by the beginning of 2012. This required some sort of formal agreement between Russia and the US, and although preparations began quite quickly following the meeting in Washington, DC, it was not finished until 2012. The draft agreements on bilateral CBMs in cyberspace were prepared for the meeting of President Putin and President Obama on June 18, 2012 on the margins of the G20 Summit in Los Cabos, Mexico. Yet, they were neither signed nor ever discussed by the Presidents during their meeting. The reason was quite trivial though disappointing: the two sides of the bilateral working group failed to agree on the final text before the meeting.

Nevertheless, work on the bilateral agreements did not stop after Los Cabos, and continued even at the start of the gradual evaporation of the US-Russian

Reset in 2012. After a series of negotiations, a terminological compromise was finally achieved (and it was the Russian phrase “the use of ICT”). After the one-year delay, the bilateral initiative was brought to a successful conclusion. A set of agreements was finally signed on June 17, 2013 at the meeting of President Obama and President Putin at the G8 Summit in Lough Erne, Scotland. More specifically, three agreements on CBMs were signed, and a Joint Statement of the two Presidents was adopted after the meeting. The Joint Statement referred to the “issues of threats to or in the use of ICTs in the context of international security”. As the US term “cybersecurity” and the Russian term “international information security” proved controversial to both, this diplomatically brilliant, though vague definition, now serves as a compromise solution for negotiations on politically sensitive issues related to the ICT between Russia and the US.

The Statement summarised the outcomes of the Presidents’ meeting. While all details were put on paper in three agreements signed by President Putin and President Obama, each of the agreements was to focus on a particular mechanism of CBMs in the field of the ICT security.

The first agreement advocated the establishment of a direct secure voice communication link between high-level officials in the White House and the Kremlin with the purpose of ensuring the effective management of potentially dangerous situations “arising from events that may carry security threats to or in the use of ICTs”. The agreement identified the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council as the primary decision-makers who would use the hotlink. The concept of the hotlink and its initial functionality were based on the experience of the Cold War era. Initially, the first hotlink was created in 1963, soon after the Caribbean crisis, when the need for a reliable, instant and direct channel of communication between decision-makers was necessitated by the threat of a nuclear war. Since 2008, the modernised hotlink was operating on the basis of a dedicated computer network, and also provided secure voice communication channel. Instant online chat and email functions became available as well. In 2013,

its purpose and the scope of functions have been expanded to include the issues mentioned in the bilateral agreement on the CBMs in cyberspace.

The second agreement was dedicated to the authorisation of the use of the 24/7 direct communication link between American and Russian Nuclear Risk Reduction Centers (NRRCs). This was envisaged to facilitate the exchange of urgent communications that would reduce the risk of misperception, escalation and conflict. Just as in the case of the aforementioned hotlink, this agreement advocated for the adaptation of the bilateral mechanism established in the Cold War era. The channel of urgent communication for the prevention of nuclear war was established in December 1987 when the American and Russian NRRCs were created. According to the agreement of 2013, the communication link involves 24/7 staffing at the Ministry of Defence in Moscow and the Department of State in Washington.

The main purpose of these two communication channels was to enable the parties to the agreements to explain their activities and/or incidents that would have otherwise been construed as a threat by the other. For example, the communication links could be used by one party to notify the other of cyber-exercises that were being held in order to avoid creating the misperception that a cyber-attack was being launched. Another important objective was to avoid creating misperceptions of actions and/or incidents related to the activities of third parties or proxy actors. For example, Party A might warn Party B about a cyber-attack targeted at Party B (or to its infrastructure/ assets or citizens) but routed through the territory or infrastructure of Party A.

One more noteworthy detail of the hotlink arrangements is their clear connection to the Cold War period mechanisms that facilitate urgent communication on strategic nuclear security issues between the two superpowers. The functions of the Russian NRRC have been undergoing the process of expansion since the Treaty on Conventional Armed Forces in Europe (CFE) was signed in 1990. In October 2013, Russian Foreign Minister Sergey Lavrov commented on a new US-Russian bilateral agreement on modification of the original

Agreement on NRRCs from 1987, stating that “the time has come to adapt the NRRCs to the new realities”. This just reminds us that today, both Russian and US hard security experts and decision-makers see the ICTs as equal to WMDs in terms of its influence on global security.

The third bilateral agreement focused on fostering cooperation of the national Cyber Emergency Response Teams (CERTs). The agreement, in fact, made a precedent for permanent and systematic exchange of data between Russian and US CERTs. In particular, it suggested the establishment of a communication channel as well as information sharing arrangements between the US and Russian CERTs. While the organisation in charge of the US CERT is located in the Department of Homeland Security, there seems to be no information on the controlling agency of the Russian CERT.

Finally, the mechanism of bilateral cooperation on CBMs in cyberspace would not have gained enough efficiency and enhancement potential without the establishment of a new dialogue platform. Such a platform was also negotiated as a part of the Lough Erne agreements. It was the 21st Working Group on Threats to and in the use of ICTs in the Context of International Security. The Group was established, and started its activities in the fall of 2013 under the US-Russia Bilateral Presidential Commission. This, in turn, was launched in 2009 as a major component of the US-Russia bilateral relations Reset.

The Working Group comprised of two delegations: Russian and American. Accordingly, one co-chair was appointed from each side. The US Co-Chair was Michael Daniel, Special Assistant on Cybersecurity to the President of the USA – or just “the Cyber Czar”. The Russian side delegated Deputy Secretary of the Security Council of the Russian Federation Nikolai Klimashin as co-chair. But the most experienced expert in cyber-issues among Russian members of the Group was Andrey Krutskikh, then Special Coordinator of the Ministry of Foreign Affairs for the Political Use of ICTs. In February 2014, Mr. Krutskikh was appointed Special Representative of the President of the

Russian Federation for International Cooperation in Information Security, thus defending his own informal title of “the Russian Cyber Czar”.

Moscow and Washington formulated the purpose of the new expert dialogue site as follows: “to assess emerging threats, elaborate, propose and coordinate concrete joint measures to address such threats as well as strengthen confidence”. The working format was based on regular meetings and discussions of the members of the Group.

The inaugural meeting took place on November 21–22 in Washington, and its agenda included:

1) Development and implementation of the bilateral CBMs
2) Regional scope: finding ways to promote regional CBMs in venues such as the OSCE and the ASEAN Regional Forum (ARF)
3) Discussion of norms of state behaviour, cooperation to combat crime in the use of ICTs, and defence issues resulting from the use of ICTs

The author was not able to find any open source information about possible further meetings of the Working Group. One of the meetings was probably scheduled for the spring of 2014. Unfortunately, deterioration of US-Russian relations in the light of the escalation of the Ukrainian crisis has affected the bilateral collaboration in the field of ICT security as well. In April 2014, the activities of the Bilateral Presidential Commission including the Working Group on Threats to and in the Use of ICTs in the Context of International Security were suspended. Nevertheless, this did not imply the denouncement of the bilateral agreements on the CBMs, which were still in force at the beginning of August 2014.

Unclear future of the bilateral breakthrough

At the moment, the bilateral agreements are still in the process of

implementation, so it would be premature to assess their impact on strategic security in terms of the use of the ICTs, or to speculate on their efficiency. In fact, the technical implementation of most of the CBMs suggested by the agreements started at the end of 2013, and thus, they have functioned for less than a year. Since the moment they were signed, there were not many public comments on their efficiency or any other substantial feedback from representatives of the US or Russian authorities.

In June 2014, the Special Representative of the Russian President, Mr. Andrey Krutskikh, revealed in an interview on *Kommersant* (a leading Russian newspaper), that the US-Russian agreements on CBMs might be considered "a non-aggression pact for cyberspace". He also characterised them as "unique and absolutely practical". He also confirmed that the information exchange mechanisms had already passed technical testing, and had proven to be effective. Apparently, they had been used during the preparation and conduct of the Winter Olympic Games in Sochi in February 2014, and the Russians were satisfied with the results.

At present, the future of the bilateral agreements and the future of US-Russian bilateral dialogue on information security issues seem fragile and unclear. The Ukrainian crisis has turned out to be a serious challenge for bilateral collaboration in the security field. But the question is whether the decay of bilateral cooperation on ICT security and CBMs is the only option – the likely answer is "No".

A possible reason for that is the growing vital necessity of the international community to control the use of ICTs for military and strategic purposes; almost to the degree it took in relation to the WMDs during the Cold War. There is a chance that cybersecurity will play a similar role of a "top priority security basket" in bilateral and multilateral relations among the key cyber-powers, including the US, Russia and China. But to avoid conflicts in cyberspace we need to develop "safety nets" of bilateral mechanisms such as the US-Russian agreements on CBMs, and to do it in a strategic manner, notwithstanding current political fluctuations and crises.

The Role of Civil Society in Furthering CBMs

The Role of Civil Society in Furthering CBMs

Daniel Stauffacher

We are undoubtedly living through a moment of significant change whereby a series of developments have led to the loss of public trust. The links between states on the one hand, and between state and citizens on the other, are being increasingly challenged by a range of state practices, including the negative uses of information communications technologies (ICTs) to advance political, military and economic objectives. Indeed, states and non-state actors are increasingly using ICTs to ratchet the advantage during armed conflict or situations of tense political contestation.

This situation has emerged at a moment of broad and complex shifts in the post-cold war international order, solutions for which are proving difficult to shape. It has also emerged at a time when citizen trust in the behaviour of state actors (and politicians) has decreased considerably. Evidence of this mistrust became manifest in the calls for more enhanced democratic representation and more effective government across regions as the first decade of the 2000s drew to a close, and has been somewhat aggravated by the recent revelations of the unchecked monitoring and surveillance practices of a number of governments, democratic or not.

Notwithstanding, for several years a number of states have been engaging in a series of policy discussions over norms, confidence and capacity building measures aimed at lowering risk and building trust among states with regard to the use of information and communications technologies (ICTs) in the context of international and regional security. In 2013, representing a major breakthrough in what had heretofore been difficult negotiations, a UN Group of Governmental Experts (GGE) and the Organization for Security and Cooperation in Europe (OSCE) reached initial agreement on the nature of some of these norms, confidence and capacity building measures. Substantive discussions on how these should be applied and implemented

remain, however, at an early stage. Moreover, many of the on-going efforts to reach consensus have run into difficulty not least because it is hard (yet not entirely impossible) to fit ICTs into traditional security paradigms. Yet, most governments acknowledge the role norms and CBMs can play in strengthening trust between states and within states. In addition, core governance principles such as participation, transparency, and accountability can help build and deepen trust between states, and between states and citizens. To this end, governments have acknowledged the need to build trust and deepen their engagement with other groups – including civil society organisations – as they move to further shape and implement new norms and rules in this area.

Civil society engagement on international governance and security matters is not new, and there are scores of examples of areas in which states have accommodated such engagement. Moreover, this engagement has helped produce positive results, with international and international humanitarian law in particular benefitting enormously from the contribution of civil society organisations. The latter has helped build confidence between and within states (often through the organisation of and participation in track 1.5 and track 2 CBM processes and by fostering dialogue between parties), as well as fostering treaties, promoting the creation of new international organisations, and lobbying in national capitals to gain consent to stronger international rules and standards. International cyber security should not be an exception. Moreover, it is an area that, by its very nature and the broad range of normative concerns involved, calls for much deeper civil society engagement than experienced in other areas.

Yet, to date, civil society engagement in the shaping of national cyber security strategies or in regional and international norms and CBM processes has been minimal, despite the fact that civil society organisations represent, along with the private sector, academia and policy think-tanks, core links in the ICT value chain and have 'normative concerns' with regard to how ICT-driven international and regional security concerns are resolved. Indeed, the expertise, knowledge and reach of these groups is fundamental to resolving or responding to many of the core technical problems inherent in the ICT

environment and many of the insecurities and mistrust that has emerged between and within states regarding the uses of ICTs.

In particular, civil society can contribute by developing strategies for their effective engagement in on-going processes, particularly with regard to supporting and monitoring implementation of the 2013 GGE Report and the OSCE's Initial Set of CBMs. The GGE Report in particular highlights a number of areas in which on-going norms and CBM processes would benefit significantly from greater involvement of civil society (as well as the private sector and academia). And while the OSCE has not identified a role for civil society (nor the ARF for that matter) in shaping or implementing CBMs, there is enough precedent in the work of that organisation to demonstrate how civil society involvement is important and can add much more legitimacy to processes, the outcome of which affect all of society. In addition to direct engagement, civil society organisations can also advocate greater transparency and accountability on the part of governments, highlighting for example, where progress has been made and calling to task national leaders when required. They can similarly work with all relevant stakeholders to deepen the technical and normative knowledge base required to inform sound policy decisions.

If approached effectively and coherently, such engagement can improve the qualitative dimension of multilateral norms and CBM processes regarding international security and state uses of ICTs, affording them greater legitimacy and sustainability. It can also help ensure that broader normative concerns are attended to, and that the right technical expertise is leveraged when solutions are being sought. Combined, the latter can help build trust between states, and between states and society.

Internet Governance: Views from the Internet Society

Internet Governance: Views from the Internet Society

Noelle de Guzman

The year 2014 marks a critical point in Internet governance. On the one hand, the United States' recent announcement that it will relinquish stewardship of the Internet's technical back-end, the Internet Corporation for Assigned Names and Numbers (ICANN), could bring forth a more globalised and inclusive model of Internet oversight. On the other, the upcoming ITU Plenipotentiary Conference, where the foundational ITU treaties will be renegotiated and possibly revised, might also bring the global resource one step closer to fragmentation and state control.

There are several factors which motivate organisations like the Internet Society to continue to advocate for decentralised Internet governance. One of these is sustainability. Underlying the Internet's immense growth and mass adoption is its open and interoperable architecture, a feature that has enabled low-barrier connectivity and innovation at the edges of the network. Integral to this end-to-end model is the collaborative approach by which Internet resources are managed – unlike other global communication platforms, there is no centralised authority for the Internet. This is reflected in the distributed and bottom-up manner by which global bodies such as the Internet Engineering Task Force develop Internet standards and protocols, as well as in the loose structural makeup of multi-actor meetings like the Internet Governance Forum.

The future of Internet governance

As underlined by the first United Nations' World Summit on Information Society (WSIS) in 2003, the Internet's growing utility to society and economy has increased the range of stakeholders who each have an interest in its

oversight. Consequently, Internet governance has become more multi-faceted, with activities that range from technical standards coordination to regulation and advocacy – an ecosystem that similarly requires the participation and cooperation of various groups and entities.

The outcome document of WSIS 2005, the Tunis Agenda, had delineated distinct and separate responsibilities for each major Internet stakeholder group. It has, for instance, recognised the authority of states in Internet policymaking. These provisions however remain hotly contested in many circles. And as the 2012 World Conference on International Telecommunications (WCIT) in Dubai demonstrated, states themselves have yet to reach a consensus on their role in Internet governance. Yet there are also indications of progress. Recent events such as the NetMundial in Brazil (April 2014) allude to the continuing efforts by governments, private sector players, technical communities, civil society groups and other entities to work together to advance the multi-stakeholder model of Internet governance.

The NetMundial MultiStakeholder Statement, a product of a two-day debate and discussion among 1,480 delegates from across the world, outlines a number of guidelines for future Internet governance. It can in some ways be considered as enhancement to existing principles in that it calls for a governance model that is not only transparent and accountable, but must enable the meaningful participation of all stakeholders, both on the discussion and the decision-making table. This means inclusiveness that is backed by policy and operating at the global, national as well as local levels. It also means addressing the interests of existing Internet users as well as those who are not yet online.

The NetMundial Statement takes a different tack to the Tunis Agenda in that it recognises the varying functions that different stakeholders have in different contexts – it allows for flexibility in collaboration, with roles being identified and agreed on according to the issues at hand. Its provisions are relevant to cybersecurity practices on two fronts:

Firstly, it calls for better coordination between technical and non-technical communities to enable both groups to better grasp the policy implications of technical decisions, and the technical implications of policy decision-making. This is relevant in areas like jurisdiction and law enforcement assistance, which still needs more involvement from network operators and software developers.

Secondly, it aims to ground efforts to ensure Internet security and stability in universal human rights principles – a demand backed by a parallel resolution released by the UN Human Rights Council in June 2014. It stressed that the rights that people have offline must also be protected online – this includes freedom of expression, such as the freedom to hold opinions without interference, and to receive and impart information and ideas; freedom of association, including through social networks and platforms; and privacy.

Balancing freedom and security

A number of challenges in Internet governance, particularly in cybersecurity, stems from the fact that cyberspace is made up of infrastructure which are physically located – and thus can be easily controlled – in sovereign jurisdictions. At the same time, it is also made up of virtual properties that defy geographic boundaries. This means that every attempt to control the Internet's physical layers inevitably has extraterritorial effects.

Online security, a concern that for institutions is closely tied with issues of sovereignty and corporate control, can at face value, be easily viewed as oppositional to the notion of an open and borderless network of networks. But it is, as many Internet stakeholder groups have pointed out, a false dichotomy. The Internet's interconnected and unfragmented space lies at the heart of its resilience and at the root of its social and economic value. Efforts to limit risks by creating 'walled gardens' would greatly restrict its current and future utility – to start, balkanising the Internet can and will cause information inefficiencies across networks.

The high degree of interdependencies on the Internet means that security needs to be approached from the perspective of managing risk – taking into account threats as well as their likelihood and impact. A good starting point is to assume that there is no absolute security – there will always be vulnerabilities, and our concept of 'secure' has to take into account residual risks that are considered acceptable in a specific context.

Balancing openness and security requires a common understanding of the problems at hand, and of where the vulnerabilities lie – is it end-user devices or user-behaviour or the infrastructure or the underlying telecoms networks – so as to determine where suitable solutions, whether these are technical, policy, economic or social, can be found.

At the same time, security paradigms should be grounded on protecting the Internet as a global asset, rather than simply on preventing perceived harm. The same properties that open up opportunities for malicious activity online – accessibility through open platforms, permission-free innovation, and its global reach – are also the ones that underpin the Internet's success and its value to users. This means that security solutions should be designed and implemented in ways which seriously considers the potential effect they might have on the 'good side' of the Internet.

The Internet has allowed us to become more efficient, it has enabled new forms of production and distribution, and has given rise to economic models such as open source software. It also has the potential to be a significant instrument in addressing social ills and other global challenges. Thus, the end goal of cybersecurity solutions should be to make the Internet more resilient. These should not undo the progress that we have made in making the Internet a beneficial tool for everyone, and should not stunt the Internet's growth and potential.

Ultimately, it is people that hold the Internet together: the usefulness and effectiveness of security measures is heavily dependent on the actions of many actors and entities. The social component of cybercrime cannot be

fixed without user engagement. Neither can tools like encryption technologies be beneficial if they are not widely adopted. It is important to consider the costs and benefits of our actions for other stakeholders – and this always entails a balancing of interests, of national security with human rights, and of economic, developmental, and other relevant concerns.

Contributors' Biographies

Contributors' Biographies

Bryce Boland
CTO, FireEye, Asia Pacific

Mr Bryce Boland is CTO at FireEye, Asia Pacific. Bryce has worked as an information security professional for over 16 years. Prior to joining FireEye, he was the Security CTO for UBS, responsible for group-wide security strategy, architecture, and driving security requirements into all technology development. He also built and ran UBS's application security programme, the security testing/penetration testing programme, and the security consulting team. In previous roles at UBS he was responsible for IT Risk Management in the APAC region, the architecture of the Security Operations Centre, and the architecture of the entitlements management systems.

Previously, Bryce worked for ABN AMRO as a technology risk management consultant, where he built vulnerability management solutions, conducted penetration tests, and consulted on security for major infrastructure and application programmes. He was also a member of the ABN AMRO GCIRT and Enterprise Network Steering Committee. He has a Master's degree in Computer Science with a thesis in cryptographic protocols.

Bryce has lived and worked in New Zealand, Australia, UK, Switzerland, and now Singapore. His passion for hacking technology began at the age of 6, soldering memory into his ZX-81 on the kitchen sink.

Cormac Callanan
Owner/Founder, Aconite Internet Solutions

Mr Cormac Callanan operates an independent consultancy company from Dublin, Ireland named Aconite Internet Solutions (www.aconite.eu), which

provides expertise in policy development in the speciality area of international cybercrime and Internet security & safety. Qualified in Computer Science he has over 20 years working experience on international computer networks and 10 years' experience in the policy area of illegal content and cybercrime activities on the Internet. He has provided training at Interpol and Europol and to law enforcement agencies around the world on the subject of emerging and developing technologies. Having travelled over 45 countries for business, he currently provides consultancy services around the world and works on policy development with the Council of Europe. He was Industry Coordinator for the 2CENTRE – Cybercrime Centres of Excellence in Training, Research and Education – www.2centre.eu.

Cormac was past-president of INHOPE – the International Association of Internet Hotlines (www.inhope.org) and CEO for 5 years. During this time the network grew to 30 member hotlines in 27 countries around the world and he successfully achieved financial support of over €3m during this time. INHOPE facilitates and co-ordinates the work of Internet hotlines responding to illegal use and content on the Internet.

He was founding Chairman of the Internet Service Provider Association of Ireland (www.ispai.ie) in 1997 which he led for 5 years until February 2003 and served as Secretary General of the European Service Provider Association (www.euroispa.org). He was founding Director of the Irish www.hotline.ie service in 1998 responding to reports about illegal child pornography and hate speech on the Internet. In addition to representing INHOPE, he has represented the Irish and European Internet Service Providers at Irish government and at EU level.

Following work on international assignment in the USA and Japan, he established the first commercial Internet Services Provider business in Ireland in 1991 – EUnet Ireland – which was sold in 1996. He has presented seminars throughout Western, Central & Eastern Europe, the Middle East and Asia and has lectured on a wide range of technology issues for many years.

Damien D. Cheong

Coordinator, Homeland Defence Programme (HDP) and Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU

Damien D. Cheong is a Research Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. He has researched and written on a variety of issues related to homeland defence, strategic communication, security studies, political violence and Middle East politics. Damien earned his PhD in Politics from Monash University (Australia). Prior to joining CENS, Damien was an adjunct research fellow at the Global Terrorism Research Centre (GTReC). He also lectured in strategic communications at Monash University from 2009 – 2010.

Oleg Demidov

Program Director, The Russian Center for Policy Studies

Mr Oleg Demidov is Director of the Program International Information Security and Global Internet Governance at the Russia Center for Policy Studies (PIR). He graduated from the School of Public Administration at Moscow State University of Lomonosov in 2010. Currently, Oleg is working on his Ph.D thesis at Moscow State Institute of International Relations (MGIMO University). In 2011-2012, he held the position of Project Coordinator at the Center for Political and International Studies (CPIS) under the International Federation for Peace and Conciliation. Since 2012, he has served as an expert to the Commission on Information Security and Cybercrime at the Russian Association for Electronic Communications (RAEC).

Since 2011, Oleg has been participating in the international project “A Twenty-First Century Concert of Powers” conducted by the Frankfurt Peace Research Institute (PRIF) (through 2014). He is the author of a number of research articles on information security, cybersecurity, and global Internet governance in the PIR Center’s Security Index journal and other editions. Oleg serves as

the Secretary of the Working Group on International Information Security and Global Internet Governance under the PIR Center Advisory Board. In March 2014 Oleg became a member of the Research Advisory Network (RAN) under the Global Commission on Internet Governance (CGIG). Oleg attends major international conferences and summits on the issues of cybersecurity and Internet governance in Russia and abroad. He speaks English fluently.

Noelle de Guzman
Regional Programmes Coordinator for Asia Pacific, The Internet Society

Ms Noelle de Guzman is the Regional Programmes Coordinator for Asia Pacific at the Internet Society (ISOC). Prior to joining ISOC, she was as a development analyst at global consulting firm Devex, and also undertook research at the London School of Economics, where she focused on media policy and regulation. Currently, she works with ISOC's Asia-Pacific Bureau to ensure that its regional initiatives are efficiently delivered and continuously monitored for impact.

Caitríona H. Heinl
Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU

Caitríona H. Heinl is a Research Fellow at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). She is responsible for research related to the CENS Homeland Defence Programme, primarily with regard to issues pertaining to cybersecurity.

She is a UK-trained Solicitor and admitted as an Attorney-at-Law in New York. She holds an MPhil in International Relations from the University of Cambridge.

Prior to joining CENS, Caitríona was the lead researcher responsible for Justice and Home Affairs policy and the Justice Steering Committee at the Institute of International and European Affairs (IIEA), Ireland. Under this portfolio, she was required to conduct analysis on a wide variety of European and international issues such as European and international criminal justice, fundamental rights, data privacy and data protection, police and judicial cooperation, crime prevention and the fight against transnational organised crime, counterterrorism, international security and cyber issues. She was the Institute's project and content editor in conjunction with former Senator Eugene Regan SC of European Criminal Justice Post-Lisbon: An Irish Perspective. Caitríona was the legal researcher and IIEA-based project manager for a study on behalf of the European Commission's Directorate-General Justice, Liberty and Security on non-legislative measures to prevent the distribution of violent radical content on the Internet including a transferability analysis of methods applied in the 27 EU Member States to prevent the dissemination of illegal content through the Internet. She was also a key member of a European Parliament funded project, providing key information to Irish citizens on the work of the European Parliament.

Kah-Kin Ho

Head of Strategic Security, Corporate Technology Group, Cisco Systems

Mr Kah-Kin Ho has been with Cisco for more than 18 years and in his current role as the Head of Strategic Security, a position he has held since January 2014, he plays a key role in developing and shaping Cisco's strategic positioning in security that aligns with customer requirements. He also serves in the Advisory group of EUROPOL European Cyber Crime Center (EC3) and teaches Cyber Security Strategy and Policy at ETH Zürich.

He was the Head of Cyber Security Business Development for 3 years where he had been involved in providing thought leadership to private and public sector organisations globally on how to respond to cyber-risk and threat.

Prior to this, he was a Solution Architect in the Global Government Solutions Group working on large defence programmes in Asia Pacific and Europe. In addition Kah-Kin had spent 4 years working with Defense System Integrators to jointly develop communications solution for the Tactical Battlefield. Kah-Kin has also filed 2 US Patents on IP Networking protocols.

Ulrich Kühn

Researcher, Institute for Peace Research and Security Policy, University of Hamburg

Mr Ulrich Kühn is a Researcher at the Institute for Peace Research and Security Policy Hamburg. He studied History at the Rheinische-Friedrich-Wilhelms-Universität Bonn. From 2007 to 2008 he worked as a Research Assistant at the Waitangi Tribunal Unit/Ministry of Justice, New Zealand. 2008 to 2009 he completed the postgradual Master's Programme "Master of Peace and Security Policy Studies" at IFSH. From 2010 to 2011 he worked as a Political Desk Officer on nuclear arms control to the Division for Disarmament, Arms Control and Non-Proliferation at the Federal Foreign Office of Germany (Ref. 240) in Berlin. In 2011 he was awarded "United Nations Fellow on Disarmament". He is a co-founder of the IDEAS network for the establishment of a Euro-Atlantic and Eurasian security community. Currently he is coordinating the project on Challenges to Deep Nuclear Cuts (www.deepcuts.org). He has extensively published on European security issues, the OSCE, the Conventional Armed Forces in Europe (CFE) Treaty, military CSBMs in the European theatre and nuclear arms control.

Cherian Samuel

Associate Fellow, Institute for Defence Studies and Analysis

Dr Cherian Samuel is Associate Fellow in the Strategic Technologies Centre at the Institute for Defence Studies and Analysis, an autonomous think tank affiliated to the Indian Ministry of Defence. He has written on various cyber

security issues, including critical infrastructure protection, cyber resilience, cybercrime, and Internet governance. He has also presented on these topics at seminars and round tables around the world as well as different fora in India. His recent publications include Cybersecurity and Cyberwar, (October 2013 issue of Seminar magazine), Emerging Trends in Cyber Security, (IDSA Web Comments March 28, 2012),and Prospects for India-US Cyber Security Cooperation, (Volume 31, Issue 2, Strategic Analysis September 2011). His monograph Global, Regional and Domestic Dynamics of Cybersecurity will be published shortly. He was co-ordinator of the IDSA Task Force on Cyber Security which published a report on "India's Cyber Security Challenges" in March 2012.

Daniel Stauffacher

President, ICT4 Peace Foundation

Former Ambassador of Switzerland, Daniel has a Master's degree in International Economic Affairs from Columbia University, New York and a Ph.D. in copyright and broadcasting media law from the University of Zürich. He worked for the district court of Zurich and was Managing Director of a publishing company, before joining the United Nations in New York, Laos and China (1982 – 1990) and the Swiss Government (1990 – 2006). For the latter he was, inter alia, responsible for the hosting and preparation of the UN World Summit on the Information Society (WSIS) that was held in Geneva in 2003 and Tunis in 2005. He was a member of UN SG Kofi Annan's UN ICT Task Force and is, among other, the Founder and President of the ICT4Peace Foundation, (www.ict4peace.org), founding Director, World Wide Web Foundation Board (www.webfoundation.org). Since 2007 he serves as an advisor to several Governments and to the UN on improving Crisis Information Management Systems (CiMS) and helped to develop the UN Crisis Information Management Strategy. Since 2006 he and his colleagues from ICT4Peace have called for and participated in international consultations and negotiations to maintain a secure, open and free cyberspace and published a number of publications to support such international processes.
(See publications: http://ict4peace.org/?p=1076).

Senol (Shen) Yilmaz
Associate Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU

Senol (Shen) Yilmaz was an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Shen read Business Law in Germany and England for his first degree and served stints in London, Stuttgart, and Tokyo. In 2008, he graduated as a Fulbright Scholar with an MA in International Relations from the Maxwell School of Citizenship and Public Affairs, Syracuse University, New York. Prior to joining CENS, Shen worked with German federal ministries as well as the United Nations Office for Drugs and Crime (UNODC) in Cairo as a Mercator Fellow on International Affairs.

ISBN: 978-981-09-3545-0

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