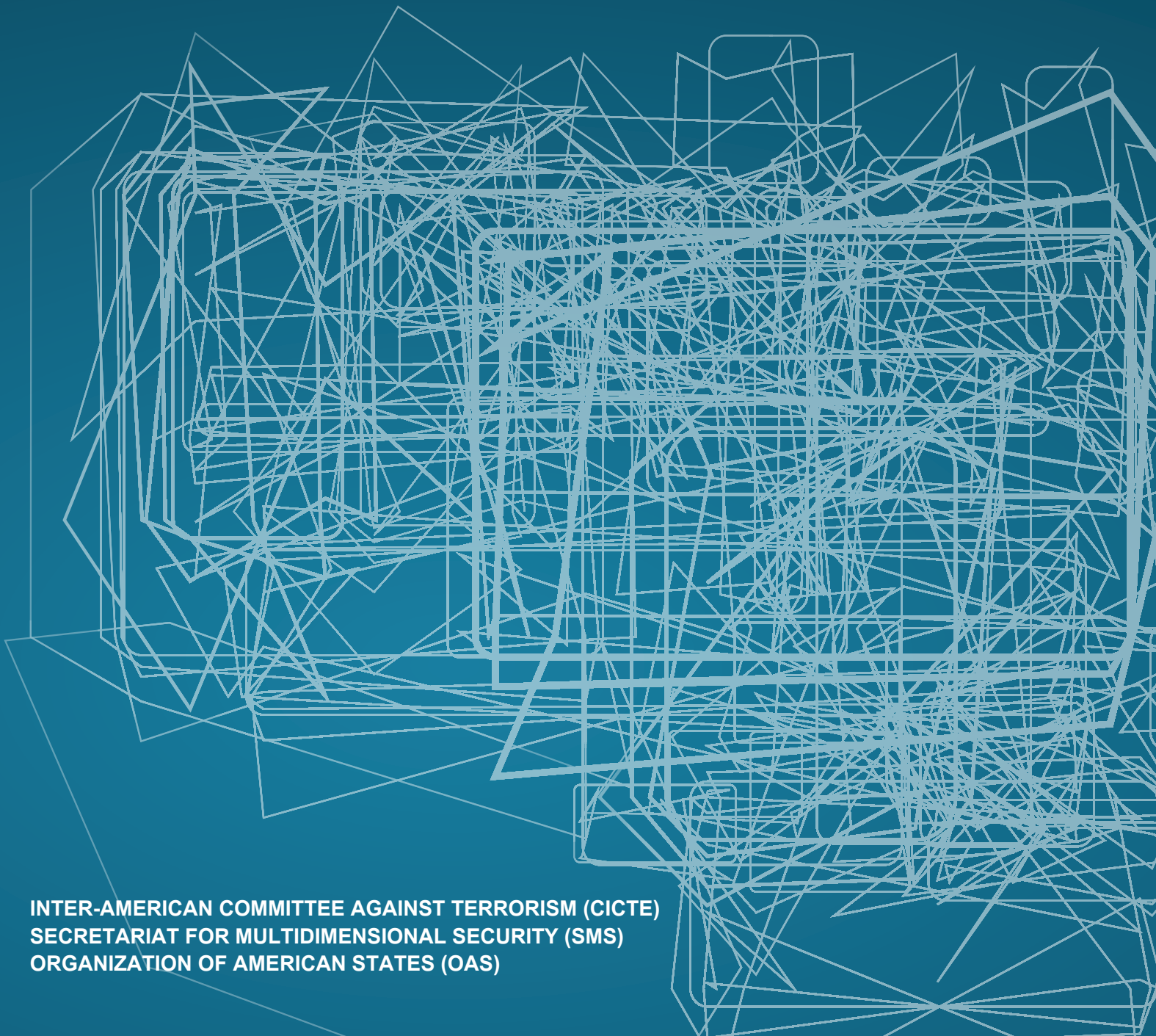
Organization of American States

CICTE

OAS CYBER SECURITY JOURNAL:
Views and Advances on Cyber Security



INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)
SECRETARIAT FOR MULTIDIMENSIONAL SECURITY (SMS)
ORGANIZATION OF AMERICAN STATES (OAS)

Organization of American States

OAS CYBER SECURITY JOURNAL

Views and Advances on Cyber Security

INTRODUCTION

AMBASSADOR ADAM BLACKWELL
Secretary for Multidimensional Security
Organization of American States

In this era of rapid globalization and technological advancement, where the internet of everything, big data and the digital economy are drivers of growth, we need to develop strategies to mitigate the risks to these networks.

In their 2004 Comprehensive Inter-American Cybersecurity Strategy, OAS Member States called for the creation of a culture of cyber security. While governments of the Americas have made tremendous progress in addressing the growing number of issues that could threaten our digital lives, much more needs to be done. In this context, the Cyber Security Program of the Organization of American States proudly presents its first collection of essays on cyber security issues from leading global cyber security policymakers.

This, our first edition, begins by focusing on policy related issues. Subsequent editions will include descriptions of technical innovations, case studies on cyber incident investigation, and academic treatment of cyber issues, all focusing on—but not exclusively—the Western Hemisphere. Indeed, in an effort to stimulate mutual understanding and relations between regions, this issue includes a piece from the Government of the Republic of Korea illustrating its vision for the future of cyber security collaboration.

We seek to promote open discussion and sharing of opinions. The articles in this publication were solicited from a variety of sources, and written without input or consultation of the Organization of American States. They do not necessarily represent the views of the OAS or its Member States.

CYBERSECURITY: A 21st Century Strategic Issue

PAUL D. NIELSEN
Director and CEO of the Software Engineering Institute at Carnegie Mellon University

Software runs the world. Year by year, decade by decade, software permeates new domains. It interconnects people and systems, becomes smarter, more complex and more autonomous. This is no random walk, but a consistent, purposeful advance for economic gain, improvements in quality of life, and for solutions to the problems we face and the opportunities we seek.

Alvin Toffler anticipated much of this change in *The Third Wave*, published in 1980. In 2005, the popular journalist Tom Friedman chronicled aspects of this advance in *The World is Flat.* More recently, in a 2011 Wall Street Journal essay, Marc Andreessen called attention to the ubiquity of software in "Why Software is Eating the World." Mr. Andreessen highlights a key point: successful, resilient organizations must now not only excel at their core business, but must also be capable *software organizations.*

As we have come to depend on software more, we face the risks that arise from this dependence. The size and complexity of software, as well as the interconnectedness of software enabled systems, mean possible exposure to disruptive, damaging events. These stem not only from software quality issues, emergent behavior, and unforeseen dependencies—but also from cyber attack by hackers, insiders, criminals, nation states, and terrorists. Size makes it more likely that software code will include vulnerabilities. This is compounded by complexity, making it more difficult to assess the impact of those vulnerabilities. Complexity also means that organizations may be impacted by emergent behavior—problems almost impossible to foresee during software development or deployment. Interconnectedness increases the "attack surface," allowing attack from vulnerabilities anywhere in the system. For instance, a single system component few are aware of, a patch installed too late, or a new application added to an existing system could all

be used by bad actors. The current trend to wireless, Bluetooth, and mobile applications has only multiplied the attack vectors.

From the Software Engineering Institute's (SEI) perspective, there are several basic issues that senior executives and government leaders should be concerned about regarding software and cybersecurity. These issues are important whether your organization uses software or develops software. Even if you do not think of your organization as a software-based organization, you need to consider how integral software is to your operations and your future. We recommend a three-pronged approach that includes a holistic assessment of risk, building resiliency into your organization to continue your mission despite adversity, and an investment in people.

First, senior executives have a special responsibility to assess the risks to their organizations and to design strategies to ensure that the organization continues to operate in the face of disruptive events. Organizations have always faced risks. Risks arise from many causes including natural disasters, market shifts, and competition. But today, substantial and uniquely nuanced risks also arise from the growing role of software.

In examining the risks to your organization we recommend a holistic view that spans both various types of threats and the life cycle of software. Often organizations concentrate on the risk from hackers, criminals and nation states attacking via the internet. There are other threat vectors, however; insiders, supply chain issues, quality issues in organically developed or modified software, and even inconsistently applied software policies applied across the organization.

Consider the threat from insiders. A rogue insider can take vast amounts of sensitive data from your internal software systems on USB drives or simply destroy data. Alternatively, for a software developer, an insider could insert malware in your products to attack your customers or discredit your company. While most organizations have firewalls and antivirus software, what internal controls does your organization have to limit damage from a malevolent insider?

Leaders should also strive to be smart software consumers. The CERT Program at the SEI has found that 64 percent of software vulnerabilities are due to common programming errors—errors that are well known and that could be eliminated by an emphasis on quality and the use of stronger developmental tools. Eliminating these errors could take a lot of "noise" out

of the malware landscape and help security analysts concentrate on more sophisticated threats. As an additional benefit, an early emphasis on quality has generally proved to reduce overall software development costs and development time.

Many businesses and government agencies have also found value in testing their systems for security-related issues before deployment. Despite the best efforts of developers, some vulnerabilities—even common, avoidable vulnerabilities—are present in delivered code, both in commercial off-the-shelf and custom-developed software as well as the patches sent out to eliminate vulnerabilities. A more advanced level of testing would include full penetration testing by organic or external experts.

Build resilience into your organization. After a holistic assessment of risks, you and your organization should recognize that your systems are already under attack and may be compromised. According to the 2013 Verizon Data Breach Investigations Report, 70 percent of security incidents were reported to the victim organization by an external party, rather than being detected internally. Two-thirds of incidents took more than a month to discover. Executives should know the resiliency needs for the enterprise. For instance, what information must be truly confidential, and how long can your systems be completely down: minutes, hours, or days? There are many outsiders interested in your organization. They may want your intellectual property, to steal money from you, or to disrupt your operations. They may want to gain personal information about your employees or customers, or they may just want to bide their time and embarrass your organization when it suits them.

Executives need to ask hard questions. If you are compromised, how will you know the effects and purpose of the attack? How does your organization protect sensitive information in storage and in transit? Where should you spend your tight security budget? Rather than being protected against just one threat or secure at a single point in time, how can you sustain the right amount of security over time? The issue of resiliency is rising in importance as executives begin to take stock of a growing set of vulnerabilities and threats.

Invest in people. Finally, despite technology advances, people are still the most critical link in innovation, operations and security. Remember what Marc Andreessen stated: No matter what your core mission is, your organization must also be a capable software organization. You need software-savvy leaders on your team. Make sure you invest in great

people—recruit them, develop them, retain them and reward them. They are your best line of defense against the innovative and talented people on the attack.

As a senior leader, you can improve your organization's cyber security posture by following this three-pronged approach: continuously perform a holistic assessment of risk, build resiliency into your organization, and invest in software-savvy people.

Sowing the Seeds of Cyber Security Together

JAESUK YUN
Director of the Korea
Internet and Security Agency

WAN S. YI
Vice President of the Korea
Internet and Security Agency

The Internet is drawing the world ever closer together. Increased connectivity has blessed humanity with unimaginable opportunity, but has come with a price. We have created the Internet, a place where people share ideas, meet others from distant lands, and conduct business just as they do offline. At the same time, we have become vulnerable to nebulous dangers that threaten to take a severe toll on society. Well-organized cyber attacks and cyber terrorism are two of the most striking examples, posing persistent threats to virtual *and* physical targets globally. Although a leader in the global ICT sector, Korea is not immune from worrying cyber trends. The country was affected by large-scale cyber-attacks in March and June 2013 targeting private financial institutions, broadcasting companies, and major government agencies. These incidents occurred in the broader context of digital financial frauds accelerating in severity and frequency, mainly through phishing and pharming schemes. Novel hacking techniques

and successful attacks place a growing emphasis on the role of KISA, the Korea Internet & Security Agency.

KISA has earned a reputation as a respected leader in cyber security both inside and outside Korea. One of its principle initiatives focuses on developing high caliber cyber security centers as part of the Korea Internet Security Center initiative, or KISC. Composed of three divisions totaling almost 200 people, the KISC has devised a number of cyber incident response systems and led efforts to integrate and harmonize public and private sector security programs. KISA has incorporated KISC initiatives into a larger project promoting general internet usage, personal information protection, effective responses to spam email, and Internet ethics. We would like to contribute some of KISA's lessons learned with others working in the field to enhance our collective cyber security.

Cyber security can be broadly categorized as responsive or preventive. Incident response requires culling threat and attack information from diverse sources as quickly as possible. Complex monitoring systems collect vast amounts of information that requires analysis and sharing. This, in turn, creates a need to put in place pre- and post-analysis systems designed to comprehensively assess gathered data. Only after analyzing information can technicians respond to cyber-attacks quickly and effectively. The results of data collation and evaluation of threat information should be widely shared through an open, distributed system to proliferate knowledge regarding possible attacks and threat vectors.

Prevention, particularly guarding Critical Information Infrastructure, or CII, is equally important to response. We refer to CII as a network that transmits information crucial to national security, public safety, financial systems, or any other service essential to daily life. Countless services and processes depend on CII; even a slight disruption could cause serious consequences. The implications of CII failures highlight the urgency to protect it. The 2013 Tallinn Manual, which set a milestone by presenting rules on cyber warfare, outlines the background and norms for adequate measures to protect CII.

Before the Tallinn Manual was published, a growing chorus called for guidelines on cyber warfare, specifically regarding critical infrastructure targeting. Many believed the Geneva Convention, outlining norms that prohibit attacks on non-combatants, applied to the digital realm as well. Research and production of the Manual, which was published by NATO in March 2013, commenced following the attacks that disrupted and paralyzed major infrastructure of the capital of Estonia, Tallinn. In response to this act

of cyber terrorism and with the support of the Red Cross and U.S. Cyber Command, NATO set up the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn to discuss potential guidelines on cyber warfare.

The Manual maintains that international humanitarian law is applicable to cyber warfare, suggesting, for example, that non-military objects that should not targeted. It also demands that damage resulting from cyber-attack be controlled and minimized. While cyber attacks levied in response to hacking are permitted, the Manual only permits physical counterattack if an incident from the digital realm claimed lives in the real world. The Tallinn Manual highlights the most fundamental lessons to be learned regarding Critical Information Infrastructures. Given inherent vulnerabilities of most CII, it is vital to persistently monitor them to decrease the chances of destructive cyber terrorism.

What comes before response and prevention efforts, however, is the longer-term requirement to build cyber security foundations in society. In this respect, countries must develop cyber industry by stimulating demand for information protection and fostering globally-oriented enterprises. Second, it is necessary to nurture and cultivate cyber security professionals. KISA, for example, operates a range of educational programs to develop expertise. In one such program, employers identify skilled incident response technicians who are then trained to become professional lecturers in information security. Third, cyber laws and regulations should be improved to stay current in the rapidly changing cyber security environment. And domestic and international collaboration is a must. Without cooperation, all potentially impactful measures will be ineffective and exist without proper context. KISA invests heavily in international cooperation and endeavors to strengthen collaboration with Korea's neighboring countries and strategic partners like China, Japan, the U.S., and the U.K., in addition to transnational security enterprises.

KISA recognizes that ICT is critical for the future of all countries, and accordingly shares its practical knowledge and skills with numerous developing countries. An illustrative case is the K-LINK Program, which facilitates visits of officials from developing countries to KISA for training in a range of relevant topics in ICT. Subjects include ICT policy, radio management, digital convergence, and cyber security. From the beginning of the program in 1998 to late 2012, nearly 5,000 people from 150 developing countries participated in the initiative. In the last year, an increasing number of countries has expressed a desire to work with KISA on

improving their technical and political cyber security capabilities. Complementing the bilateral partnerships we have developed, KISA is also leading the creation of the Global Cybersecurity Center (GCC) with the World Bank. Scheduled to begin operations in 2014, the GCC is the product of a concerted push by the Korean Ministry of Science, ICT, and Future Planning, to improve global cyber capabilities. Once open, it will provide considerable help for many countries and organizations in need of better cyber security.

Cyber security does not respect regional or national boundaries and has emerged as a critical issue that requires our immediate attention. The transnational complexity of cyber security means success will only come with cooperation. All nations and stakeholders must take appropriate response and prevention measures and create rich ground from which the seeds of cyber security can sprout, thrive, and bear fruit. As an organization that has experienced and successfully responded to innumerable cyber security threats, KISA is willing to share its practical knowledge and skills. These are based on extensive firsthand experience in many fields including personal information protection and response to spam email. KISA will do its part in this elaborate ecosystem to ensure the seeds of cyber security grow healthy so the real and virtual worlds reap the fruit of united efforts.

CYBERSECURITY:
A National Response

Honourable Phillip Paulwell, M.P.
Minister of Science, Technology, Energy and Mining of Jamaica

The National Development Plan “Vision 2030” articulates Jamaica’s vision as being “the place of choice to live, work, raise families and do business”. The Plan, which signals the new paradigm for the country’s sustainable prosperity, recognizes Information and Communications Technology (ICT) as being one of the most important enablers for the achievement of this vision. Underpinning the vision is an ICT Policy which provides a blueprint for, inter alia, utilizing ICT to increase Jamaica’s competitiveness.

The Government has recognized, however, that in promoting policies to increase the use of ICT it has to be mindful of not only the potential dangers inherent in its use, but also the role it has to play in building trust and confidence. Moreover, the government is cognizant of the fact that for the average person, consideration of these issues is likely to be limited by pressing physical crimes committed on terra firma.

Accordingly, the Government commenced the process of establishing a legislative framework through the promulgation of several pieces of legislation aimed at promoting trust, confidence and security. These include the Electronic Transactions Act, the Cybercrimes Act, the Child Pornography Act and the Law Reform Act. The Cybercrimes Act, in additiona, created offences addressing unauthorized interception, computer system sabotage and unauthorized access and enabled the investigation and prosecution of same.

Further, to ensure the Act remained in line with international best practice and appropriately addressed new and emerging cyber threats, a Joint Select Committee of both Houses of the Jamaican Parliament was established to review the legislation. The Committee having completed its review has recommended, inter alia:

a) The introduction of new offences such as forgery, fraud and malicious communication; and
b) Significant increases in penalties, with a view to signalling to cyber criminals the seriousness with which this issue is being treated.

Notwithstanding the legislative progress that has been made, the Government is aware that there are other elements that are critical to establishing a culture of trust and a sense of security in cyberspace. It recognizes that as policy-maker, it has a responsibility to provide strategic direction and to enunciate policy statements regarding cyber-security to ensure that there is mutual understanding of the cyber-security issues and a shared vision for addressing same.

While the ICT Policy identifies a few strategies with respect to cyber-security and the National Security Policy recognizes that there are potential threats to cyber-security and ranks cybercrimes as a Tier 1 threat with a high probability and high impact, there is at present, no documented strategy for cyber-security. The effect is that there is no coherent or cohesive plan to, inter alia, respond to threats and incidents. For this reason Jamaica, with

the assistance of the Organisation of American States, will shortly commence work on the development of a strategy.

The introduction of a framework to detect and address cyber-attacks and threats is a critical pillar of any cyber-security plan. It is reported that in 2004, Argentina, Brazil, Canada, Chile and the United States of America were the only countries in the Americas with national Computer Incident Response Teams (CIRT). In 2011 there were eighteen CIRTs; however of that number only two were in the Caribbean, a region which comprises over a third of the number of countries in the Americas.

The Jamaican ICT Policy, in addressing the matter of the utilization of ICT for enhanced national security, identified as a strategy, the establishment of a CIRT. To this end, Jamaica has engaged the assistance of the International Telecommunication Union to establish a national CIRT and aid in the building and deployment of related technical capabilities.

By far the most immediate problem identified in the majority of developing countries is the urgent need for capacity building in the area of cyber-security. While there exists, in Jamaica, a cadre of professionals with the technical know-how to identify, diagnose and respond to cyber and other digital crimes, the numbers are admittedly insufficient. The Government, through the Jamaica Constabulary Force and the Office of the Director of Public Prosecution, has established Units (the Communication Forensic and Cybercrime Unit (CFCU) and the Digital Evidence and Cybercrime Unit respectively) responsible for investigating cybercrime and prosecuting cybercrimes respectively. Notably, the CFCU is being reorganised to form its own Division and could, with the requisite regional and international collaboration, share its resources and know-how with other countries in the Caribbean region.

The foregoing notwithstanding, there remains a need for training of other officers of the judicial system, such as Resident Magistrates and Clerks of Courts. There is also a need to train ICT professionals across Government and to educate the populace as to the threats cybercrimes pose and the steps to mitigate same. Consequently, the development and implementation of sustainable capacity building and public awareness programmes is imperative.

Therefore, to advance the work in this area, the Government has established a National Cyber Security Task Force (NCSTF) comprising a broad

cross-section of stakeholder representatives from the public and private sector, as well as, academia. The NCSTF will, inter alia,

- assist in creating a framework to facilitate the building and enhancement of confidence in the use of cyberspace and the protection and security of related assets through collaboration amongst all stakeholders;
- establish a public education and awareness programme; and
- formulate a strategy to develop, grow and retain high quality cyber talent for the national workforce.

ICT undoubtedly has the potential to enable developing countries to, inter alia, foster economic growth; facilitate social development and improve citizen participation. However, as we become more reliant on ICT, the issue of cyber-security becomes even more pertinent. To ensure the long-term development of the ICT sector and reduce cybercrimes the identified challenges must be addressed. However, as we grapple with these challenges, the trans-borderless nature makes it imperative that we co-operate at the regional and international levels, with a view to reducing its impact. Our efforts certainly can be enhanced when we find common means to tackle this increasingly problematic issue.

Trinidad and Tobago's Coordinated Approach to Cyber Security

Senator the Honourable Gary Griffith
Minister of National Security of Trinidad and Tobago

In today's globalised world, information and communication technology (ICT) and the Internet are critical tools for development. The transformative potential of ICT and the Internet has been recognized by the Government of Trinidad and Tobago which identified ICT and the establishment of a diversified knowledge economy as two discrete development pillars within its Medium Term Policy Framework 2011-2014. It is the Government's intent to promote universal and equitable access to,

and use of ICTs and the Internet, in order to bridge the digital divide and provide for the inclusion of underserved and un-served communities.

While it is an underlying reality that ICTs provide many benefits and opportunities, it is also evident that there are various risks lurking in cyberspace. In recent years, cyber attacks have emerged as a new security threat worldwide. These continue to evolve, increasing in frequency and complexity. The virtual domain of cyberspace seems to provide the ideal platform for criminals to commit attacks at relatively low costs and presents new challenges for law given the difficulty in identifying perpetrators.

New and non traditional threats to security require modifications in existing approaches towards addressing national security and the ability to constantly adapt to the changes within the international security system. Failure to adapt to such changes increases the risk of disruption to state activities which can undermine stability and competitiveness.

Due to the increasing threats within cyberspace, Trinidad and Tobago recognised the need for a coordinated approach to addressing cyber security. The Government of Trinidad and Tobago has been developing strategies to effectively reduce our nation's vulnerability to cyber threats. Our oil and gas industry, banking and financial sector and public utilities, among others, all rely on virtual processes and are susceptible to attacks which could have catastrophic consequences for the national economy. Efforts to address these threats have been ongoing since 2008 which resulted in the establishment of an Inter Ministerial Committee (IMC) in 2010. This IMC was led by the Ministry of National Security and comprised several key Ministries and state Agencies. It was tasked with a specific mandate which included inter alia, the development of a National Cyber Security Strategy, the facilitation of the enactment of a National Cybercrime Act and the creation of a Computer Security Incident Response Team (CSIRT).

The National Cyber Security Strategy guides all cyber security initiatives and operations within the country. In implementing the measures therein, the Government of Trinidad and Tobago will create a secure and resilient cyber environment which would allow for the exploitation of ICT for the benefit and prosperity of all. The Strategy takes a multi-pronged approach to address cyber security by focusing on five (5) pillars:

1. **Governance:** The Government has envisioned the creation of a Trinidad and Tobago Cyber Security Agency (TTCSA) to function as

the main entity responsible for the coordination of all cyber security matters. The TTCSA would not perform a law enforcement or intelligence gathering role but would work closely with the Units responsible for said activities.

2. **Incident Management:** Like many states throughout the world, Trinidad and Tobago acknowledges the requirement for a mechanism to provide watch, warning and recovery services to secure and strengthen our critical information infrastructure. In this regard, a Trinidad and Tobago CSIRT is currently being established which would serve as the national focal point for incident reporting, management and response.

3. **Collaboration:** Cyberspace is a shared responsibility. Therefore cooperation among all stakeholders, particularly the private sector will continue through information sharing and other activities. Relationships with international organisations and other countries would also be bolstered as this nation is willing to share its experiences and learn from the mistakes and best practices of others.

4. **Culture:** Awareness is a pre-requisite for effective protection in cyberspace. In collaboration with the private sector and academic institutions, awareness raising campaigns would be conducted to educate all stakeholders, including the general public on security in cyberspace. Training and capacity building is also a priority as the nation seeks to increase the number of certified ITC security professionals.

5. **Legislation:** In recognition of the need for enabling legislation to adequately fight cybercrime, Trinidad and Tobago has drafted a new and more robust Bill to deter and prosecute such offenders.

Through these five pillars, the National Cyber Security Strategy would ensure the availability, integrity and confidentiality of all systems while harnessing the potential for economic growth and development facilitated through ICT and the Internet and protecting the privacy of all users.

The Prime Minister of Trinidad and Tobago has lead responsibility for security in the Caribbean Community (CARICOM) quasi-Cabinet. In this regard, the country aspires to be a regional leader for cyber security as it continues to build capacity and modernize its approaches towards law

enforcement and crime fighting. Cyber security is therefore a priority for the Government and we remain committed to working with our global counterparts in combating threats to cyberspace.

The Technology Revolution in Uruguay

Jose Clastornik
Executive Director of the Uruguayan Agency for E-Government and Information Society (AGESIC)

The development of information and communications technology (ICT) has implied significant challenges and changes for society. As people seek to adopt and widely employ ICTs, they will realize that a paradigm shift is needed. This shift, precipitated by technological evolution, is influenced by better access to information and the democratization of knowledge, improvements in quality of life, and changes in the very way that humans interact with one another.

In today's global environment, one which connects people through ICTs and affords them new ways to manage their personal information, a new challenge to equality arises based on information access, digital literacy, citizen participation and the reduction of digital gaps.

The secure use of IT in society follows a historical model of the needs the individual has always sought in a society. Security awareness has the ability to build trust, a fundamental pillar that must guide and support the digital age.

Technology is a phenomenon that does not self-regulate; it depends fundamentally on human elements. Risks and threats are an inherent part of IT, including electronic fraud, identity theft, industrial espionage, and abuse or mismanagement of IT systems by governments.

To maintain trust in a society, governments must take measures that, to the extent possible, ensure security relative to the risk factors are inherent to IT.

In this context, the strategy endorsed by Uruguay's Agency of e-Government and Information Society (AGESIC) promotes, in addition to inclusion, ownership and the good use of IT.

Indeed, one of the principles of the new Public Administration Management System was to include and recognize the citizen. Technological evolution and the increasing ubiquity of the internet constitute a turning point in how societies develop and the role that information and communications technologies play in the people's lives. Since its establishment in 2007, AGESIC's initiatives have aligned with the Public Administration Management System and sought to empower the citizen, recognizing them as an active part of the innovation process.

Uruguay's e-Government strategy has promoted measures that encourage the secure use of IT. Technology should be accessible to all citizens, but people must trust in and have access to secure and reliable systems.

Since its creation, AGESIC has developed a comprehensive strategy, one which incorporates legal and institutional frameworks, technology infrastructure, capacity and operational development, and institutional cooperation.

The drive to implement novel actions requires the creation of a legal and conceptual framework. The sustainability of an Electronic Government and widespread confidence in IT is not possible without infrastructure and an enabling regulatory framework. Moreover, official frameworks will allow the public to better integrate ICT as an essential part of raising their quality of life.

Recognizing the importance of secure networks, in 2008 the National Response Center for Information Security Incidents, CERTuy, was created by law as a body within AGESIC. The aim of the Center is to regulate the protection of critical information assets of the State, to disseminate cyber security best practices, to centralize and coordinate incident response, and to take preventive security measures when necessary.

In addition to incident management, CERTuy has led a number of projects, including creating and implementing government-wide information security policies, deploying and managing security for the national Government Data Network (REDuy), establishing a high speed network that connects the Uruguayan government and enables secure information exchange, establishing the National Infrastructure for Digital Signature (PKI Uruguay), which enables the use of advanced electronic signatures in the country, and

creating and evaluating the security in the development models of all federal ministries. CERTuy also hosts trainings with international organizations. In 2013, for example, it hosted an advanced cyber investigation training with the US Secret Service and the Organization of American States (OAS) and an advanced incident response training with the OAS and ICANN. Showing its role as a regional leader, the CERT also hosted with ITU-IMPACT a regional cyber exercise and a hemispheric event on national cyber security strategy development, again with the OAS.

The Regulatory and Control Unit of Personal Data (URCDP) was created by law, further demonstrating Uruguay's commitment to privacy personal data protection.

Subsequently, Uruguay acceded to Council of Europe Convention No. 108 on the protection of individuals and automatic processing of personal data, which was originally signed in January 28, 1981 in Strasbourg. Uruguay also adopted the Convention's associated Protocol, which seeks to ensure privacy vis-à-vis automatic personal information processing. The overarching objective of the Convention is to guarantee the respect of the fundamental rights and freedoms of people, notably their right to a private life, by ensuring privacy in regards to automatic personal data processing. The European Union has declared Uruguay in line with Directive 95/46/CA, which gauges personal data protection. The recognition by the EU shows an appreciation for Uruguay's ability to address challenges to comply with the Union's controls on the use of personal data and the work done by the URCDP.

In the sixties, the communication theorist Marshall McLuhan imagined a future in which people communicated electronically. Fifty years later, the digital age is a social phenomenon that poses new challenges in access to information, security of networked data, and the democratization of knowledge, but above all else, the improvements in people's quality of life.

Organization of
American States

Disclaimer

The contents of this publication do

policies of the OAS or contributory organizations.

Aviso importante

Los contenidos de esta publicación no

de vista de la OEA o de alguna de las organizaciones contribuyentes.

February 2014/ Febrero de 2014

1889 F Street, N.W.,
Washington, D.C., 20006
United States of America

www.**oas.org/cyber/**

OAS CYBER SECURITY JOURNAL: VIEWS AND ADVANCES ON CYBER SECURITY

Executive Secretary of the Inter-American Committee against Terrorism (CICTE)
Neil Klopfenstein

OAS/CICTE Cyber Security Program
Belisario Contreras
Brian Dito
Diego Subero
Francisco Javier Villa
Kerry-Ann Barret

Graphic Designer
Esperanza A Ramos Barajas