

# Global Cyber Expertise Magazine

## Singapore's approach to CCB

A rules-based system  
for cyberspace

-page 20-

## Cybersecurity in Ukraine

National Strategy and  
international cooperation

-page 26-

## Defining a global agenda

The next steps  
towards the GCCS

-page 35-

## CYBER CRIME AND CYBER SECURITY TRENDS IN AFRICA

Report by the African Union  
Commission and Symantec

-page 4-



**OAS** | More rights  
for more people

## **Editorial**

## **Regions**

### **Africa**

- 4 The “Cybercrime and Cyber Security Trends in Africa” Report
- 7 The African Union Commission and Internet Society Support Internet Infrastructure Security in Africa

### **America’s**

- 10 Raising cybersecurity awareness by building trust through transparency
- 13 Data protection laws and cybersecurity: Challenges for Latin America

### **Asia & Pacific**

- 16 Introducing the Cybersecurity Alliance for Mutual Progress (CAMP)
- 20 Singapore’s approach to international cyber cooperation

### **Europe**

- 23 The EU’s efforts in fighting cybercrime: Putting together legislative action, cross-sectoral and international cooperation, as well as capacity building
- 26 Cybersecurity in Ukraine: National Strategy and international cooperation

## **Global developments**

- 29 A trusted cyber foundation for the Fourth Industrial Revolution
- 32 Interview: Alexander Klimburg on the Global Commission on the Stability of Cyberspace
- 35 Working towards a global cyber capacity building agenda in 2017

# Editorial



Welcome to the third issue of Global Cyber Expertise Magazine!

A joint initiative of the Global Forum on Cyber Expertise, the African Union, the European Union, and the Organization of American States, this magazine is aimed at providing to cyber policymakers and stakeholders an overview of key developments on global cyber capacity building policies and activities.

This third edition covers a wide range of topics that touch upon both thematic challenges and responses to cybersecurity as well as regional updates and initiatives across the cyber spectrum.

Our cover story comes from Africa where a flagship study on the cyber threat landscape in the continent has been published as a collaborative project by the African Union Commission and Symantec which also marks the successful completion of one of the very first initiatives announced at the launch of the Global Forum on Cyber Expertise in 2015. The joint work of the African Union Commission and Internet Society is also highlighted with information on the recent guidelines on internet infrastructure security.

From the Americas we have a reflection on how a multi-stakeholder approach to the development of cybersecurity policies and strategies can positively impact on increasing the public's trust to the internet, while an analysis on the situation of data protection regulation vis-à-vis cybersecurity is also provided in comparison to the European and American acquis. On the other side of the globe, the Korean initiative to create a Cybersecurity Alliance for Mutual Progress comes in response for effective partnership frameworks in addressing cybersecurity challenges, while our article from Singapore demonstrates the inter-linkages between cyber norms, responsible state behaviour in cyberspace and capacity building. With regards to Europe, we have an interesting, comprehensive review of the progress made in Ukraine in the area of cybersecurity governance since the high-level attacks of 2015, as well as an overview on the European Union's approach in addressing cybercrime.

At the same time, with the global community preparing for the Global Conference on CyberSpace to be hosted by India in late 2017, the Global Forum on Cyber Expertise is elaborating its plans for the facilitation of a discourse amongst experts and partners in the Global North and the Global South towards defining a shared global agenda on cyber capacity building. Other updates with the global dimension include the setting up of the World Economic Forum's new Center for the Fourth Industrial Revolution, as well as the establishment of the Global Commission on the Stability of Cyberspace which will endeavor to develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

We value your feedback and would welcome your suggestions and contributions for the next issue. We therefore invite you to share with us information on developments in your countries and organisations, as well as upcoming cybersecurity events such as conferences, workshops, training events to feed into the next global agenda.

In thanking our guest editors, we hope that you will find the updates of this issue useful and look forward to your ideas!

On behalf of the Editorial Board,

## **Nayia Barmaliou**

Policy Coordinator and Programme Manager, Organised Crime and Cyber  
European Commission, Directorate General International Cooperation and Development

# The “Cybercrime and Cyber Security Trends in Africa” Report

A seminal benchmark for African Union countries on the path to cyber security confidence

With a young population that is rapidly adopting new technologies, a pattern of ICT development that has leap-frogged infrastructure-reliance and a burgeoning e-commerce industry, Africa’s economy is poised to grow. But prosperity and digitization come with new risks and vulnerabilities, such as cybercrime, that could undermine progress. To better understand the cyber threat landscape in the continent, the African Union Commission and Symantec released a report analyzing cyber security trends and government responses in Africa, as part of a Global Forum for Cybersecurity Expertise Initiative with support from the U.S. Department of State. The report explores various cyber security trends in Africa, including the overall professionalization of cybercrime, while it also takes stock of the many advances made by national governments.

Written by: Ilias Chantzios, Senior Director of Global Government Affairs for Europe, Middle East & Africa (EMEA) as well as Asia Pacific and Japan (APJ); Global Advisor for Critical Infrastructure and Data Protection at Symantec Corporation and Moctar Yedaly, Head of Information Society Division, African Union Commission.

## The African cyber paradigm: opportunity and vulnerability

While the African continent is fast developing its ICT infrastructure in all its dimensions, thanks to a

growing economy, it has also become more vulnerable to cyber threats. Africa has leap-frogged many cycles of technological advancement, for instance in terms of telephone landlines vs. mobile telephony, and today finds itself in a situation where ICT, mobile connectivity, social media, and even the Internet of Things (IoT), be-

come formidable vehicles of growth and modernisation, as well as targets for internal and foreign investment.

Africa has a young population -in fact the youngest of the world- with a median age just below 20 years[1]. Young generations are embracing the features of today’s social engagement, hyper-connectivity,



*Cybersecurity & Cybercrime Trends in Africa Report, Symantec and African Union Commission. Credits: © 2016 Symantec Corporation*

and automation, both at work and in their personal lives. At the same time, however, all this puts Africa in the same range of cyber vulnerability already experienced by other regions with more sophisticated technological environments, especially when it comes to cybercrime.

Cybercrime is on a dramatic rise on a worldwide basis, and Africa is not immune from it. In order to carry out their activities, cyber criminals look for fertile environments, both in terms of technological vulnerability and user behaviour. As an example, Africa is the leading force for mobile money transfers: 14% of all Africans receive money through this medium[2]. Further, the e-commerce business is estimated to reach a market value of \$75 billion by 2025[3]. This immediately becomes an enticing proposition for increasingly sophisticated cybercriminals, who, like everywhere else in the world, exploit both vulnerable technology and users' carelessness.

Moreover, outdated operating systems further compound the situation. Indicatively, about 25% of personal computer users in Africa are still on Windows XP[4] that were first released in 2001 and today unsupported and unpatched, or even pirated software. Meanwhile, in the mobile sphere, nine out of ten devices use the Android operating system which is by a long way the most vulnerable in the marketplace.

The result is a growing cyber criminality and a severe threat to the overall economy of the continent, which governments need to tackle decisively and in a timely manner to avoid a very punishing outcome and a de facto barrier to the path of advancement. However, only a three-pronged effort can contribute to an effective response:

- Policymakers will need to implement effective policies towards the creation of a safe cyber environment and the increase of confidence in the use of technology, for government agencies, businesses, and citizens.
- Technology companies can provide the necessary tools, in terms of infrastructure, devices, software and, crucially, cyber intelligence.
- For their part, users need to adopt sound habits and careful mastering of connectivity capabilities.

### Understanding the threat landscape

The borderless nature of cybercrime makes African countries vulnerable to all threats already present

**“The first report ever related to cyber incidents and illicit cyber activities affecting organizations and individuals in Africa.”**

elsewhere. In this context, African policy makers find themselves in the compelling need to develop and implement effective policies, legislation as well as awareness and education initiatives to address the risk of cybercrime and cyber threats in general. But any set of measures to be effective require a thorough understanding of the threat landscape. To this end, cyber intelligence is a crucial tool in the effort to increase cyber security and consequently confidence in the use of technology.

Symantec, as the largest cyber security company in the world, can count on the largest set of sensors on the Web, called Global Intelligence Network (GIN). Every year, hundreds of extremely skilled analysts, analyse trillions of bytes of telemetry gathered through these sensors, and distil the data into an annual report: the Internet Security Threat Report (ISTR).

In order to overcome the information gap the African Union (AU) and Symantec, through the Global Forum for Cyber Expertise (GFCE) and with the support of the U.S. Department of State (DoS), have engaged in a Pu-

—

**“The report is crucial for policy makers and law enforcement agencies to understand the cybercrime paths, motivations, targets, techniques and vehicles”**

blic-Private Partnership to develop a report that collected and presented detailed technical data on the cyber-security threats in Africa.

The report **“Cyber Crime & Cyber Security Trends in Africa”** analyses the key technological trends in the continent and the cybercrime proliferation and its techniques. The unique feature of this report is that it incorporates online threat data from Symantec’s comprehensive cyber threat monitoring network, including the GIN and the ISTR mentioned above, as well as the perspectives of African Union Member State governments. Some key findings point to the proliferation of ransomware, social media scams and the explosion of mobile malware in the continent.

The analysis of this information is crucial for policy makers and law enforcement agencies to better understand the cybercrime patterns,

motivations, targets, vulnerabilities, and techniques. The improved cybercrime threat assessment capability of governments can allow them to have an evidence-based decision making, including in the prioritisation of resources for their national capacity building efforts and in managing the cybercrime risks for citizens and businesses. As a result, this comprehensive report shall serve as a valuable tool to African governments to identify gaps, select measures and prioritise the allocation of resources in addressing the diverge range of cyber threats. This is particularly pertinent considering that both financial and human resources are limited, since cyber security skills are the scarcest in the ICT realm and not only in Africa but also globally.

—

**A collaborative endeavour**

The report was officially launched by the AU on 10 March this year, and will therefore become a useful benchmark for future endeavours and analysis in the African cyber landscape. Thanks to the strong commitment and proactive attitude of all involved stakeholders, the process in itself has been an enriching experience for all parties involved. A project full of complexity both by nature and distance, it was made possible due to effective coordination and multiple iterations amongst the different stakeholders and contributors. In this respect, the networks of the AU and DoS were instrumental to the outcome, while the GFCE proved to be a valuable forum

for mobilising relevant actors and putting together such an initiative.

The ‘Cyber Crime and Cyber Security Trends in Africa’ Report represents a ground-breaking, inspirational initiative, which can pave the way to new bold projects in the field of cyber security that can support the African governments build capacity and confidence in cyberspace and further progress on a path of economic and technological growth.

**More information:**

[1] <http://www.worldometers.info/world-population/africa-population/>

[2] UNCTAD Information Economy Report 2015

[3] <http://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa>

[4] [http://www.uneca.org/sites/default/files/PublicationFiles/ntis\\_policy\\_brief\\_1.pdf](http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf)

# The African Union Commission and Internet Society Support Internet Infrastructure Security in Africa

Cyber threats are evolving and increasing at a fast pace. African countries need to urgently scale up their efforts to effectively secure the internet and ICT infrastructures in order to enable their citizens to take advantage of the various new services offered by the internet. To this end, the African Union Commission in collaboration with Internet Society developed recently guidelines on internet infrastructure security for Africa. These guidelines recommend critical actions to be taken by various stakeholders involved in internet governance and development within the continent.

Written by: Dr. Dawit Bekele, Director of the African Regional Bureau of the Internet Society; and Ms. Souhila Amazouz, Senior Policy Officer, African Union Commission

## The African Union Convention on Cyber Security and Personal Data Protection

To address the challenges posed by criminal activities committed over ICT networks in a manner that is relevant to regional and continental spe-

cificities and in response to the need for harmonized legislation in the field of cyber security and personal data protection across the African nations, the 23rd Assembly of Heads of State and Government adopted in June 2014 the 'African Union Convention on Cyber Security and Personal Data Protection', also known as the 'Malabo Convention'.

The Malabo Convention seeks the establishment of a comprehensi-

ve continental legal framework that sets broad guidelines for electronic transactions, personal data protection as well as cybersecurity and cybercrime in the African cyber ecosystem. It embodies the existing commitments of African Union (AU) Member States at sub-regional, regional and international levels to build an information society that respects cultural values and beliefs of the African Nations, and guarantees a high level of legal and

---

**“The Malabo Convention sets out the essential security principles for establishing a credible digital environment”**



*Experts' workshop on Internet Infrastructure Security by the African Union Commission and Internet Society, 28-29 November 2016, Nairobi, Kenya. Credits: African Union Commission*

technological security to ensure respect of privacy and freedoms online while enhancing the promotion and development of Information and Communication Technologies (ICT) in the AU Member States. The Convention sets out the essential security principles for establishing a credible digital environment with a view to reduce the risks of cybercrime and abuse of personal data.

To facilitate its implementation by African countries, the African Union Commission in collaboration with Internet Society developed guidelines on internet infrastructure security for Africa. The Guidelines emphasize the importance of the multi-stakeholder model and the need for collaborative security in protecting internet infrastructure with particular focus on essential principles of internet infrastructure security in Africa. These include, most notably, raising awareness at different levels, responsibility,

cooperation, and adherence of all the concerned actors to fundamental rights and internet properties.

**Is Internet infrastructure security a critical issue in Africa?**

---

The past ten years have seen tremendous growth in the development of ICT infrastructure and internet access in Africa. From less than 5% in 2007, internet penetration reached 28% in 2015, bridging Africa's gap to the rest of the world. Since becoming available, the internet has changed the lives of many African citizens who started relying on the internet to perform daily activities such as socializing, communicating or even making money transfers through mobile phones. The example of M-PESA in Kenya

is striking as the transfer of money has allowed poor people gain access to the banking system and has also largely contributed to financial inclusion. However, the increased importance of the internet has also presented the African community with new challenges: as African citizens become connected to the rest of the world and dependent on the use of the internet and ICT, they become vulnerable and exposed to the misuse of these technologies and there is a need to ensure that the security of ICT and of the internet infrastructure is continually improved to maintain its integrity as well as internet users' trust in its reliability.

Many African countries are facing several internet-related challenges in relation to security provisions to prevent and control technological and informational risks. The major security threats affecting African organizations and individuals are either generated from inside Africa or from





Experts' workshop on Internet Infrastructure Security by the African Union Commission and Internet Society, 28-29 November 2016, Nairobi, Kenya. Credits: African Union Commission

outside the continent as part of global, sophisticated attacks. This results in users being prevented from accessing the internet and the creation of major obstacles to the use and development of the internet in the region. In particular, cyberattacks on internet infrastructure can and have cut off a whole population from access to the internet and may result in serious damage to the economy as well as threats to the security of African nations. Therefore, protecting internet infrastructures is critical in today's Africa as it is experiencing the information age revolution.

## Internet Infrastructure Security Guidelines for Africa

With internet becoming a critical component for Africa's growth, its se-

curity is vital and cannot be ensured without the collaboration of various stakeholders. In this regard, in conjunction with the Africa Internet Summit (AIS) held in Gaborone, Botswana in June 2016, the Internet Society introduced a panel discussion on internet infrastructure security in Africa. The panel allowed open discussions and came up with preliminary input from the African technical community on the scope and directions to adopt towards developing a blueprint for African countries in their efforts to protect internet infrastructure from present and future threats.

On the basis of these exchanges, the Internet Society drafted a guidelines document on internet infrastructure security for Africa which was brought forward for further discussion in November 2016 at an expert validation workshop in Nairobi, Kenya, co-organized by the Internet Society and the African Union Com-

mission. Selected experts from within and outside the continent came together to reflect over and finalize these Guidelines. Their main objective is to identify the major threats faced by internet networks in African countries and recommend the most crucial actions at organizational, national and regional levels by the various stakeholders that can support the resilience of infrastructure against cyberattacks.

## Way forward

This consultative process has led to the finalization of the Internet Infrastructure Security Guidelines for Africa which shall be publically distributed at the African Internet Summit in June 2017. Given the broad nature of internet infrastructure security, it would be opportune to complement this effort by further developing specific recommendations addressing all specific issues related to internet security, tailored to the African context.

### More information:

AU Convention on Cybersecurity and Personal Data Protection  
<https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

Guidelines on Internet Infrastructure Security for Africa

# Raising cybersecurity awareness by building trust through transparency

---

*People are increasingly distrustful of the internet, and that poses a challenge to its future. Immediate steps to enhance internet trust must be taken. Governments can restore trust online by adopting a transparent and multi-stakeholder approach to the development of cybersecurity policies and strategies. Such an approach has two distinctive advantages: first, different stakeholders can establish cooperative relations and develop a common understanding of the identified threats and the tools to counter them; and second, all parts can gain greater confidence in the ultimate approach chosen and an understanding of their role in achieving the identified objectives.*

*Written by: Megan Stifel, Cybersecurity Policy Director, Public Knowledge and Agustin "Gus" Rossi, Global Policy Director, Public Knowledge*

People are increasingly distrustful of the internet, and that poses a challenge to its future. Only 12% of the respondents of the 2017 CIGI-Ipsos Global Survey on Internet Security and Trust, strongly agree with the statement "Overall, I trust the Internet", with 65% of those who don't trust it citing security as the main reason. In Latin America, 64% of respondents are more or much more concerned about their privacy than they were a year ago.

Unless we take immediate steps to enhance trust, the internet will falter as a tool for economic growth, development, civic engagement, and the promotion of human rights. We believe that enhancing transparency and encouraging multi-stakeholder dialogues are key and necessary elements for building trust online.

## Transparency and dialogue to build cybersecurity

---

Transparency increases the understanding of cybersecurity risks and encourages governments, industry and civil society to coordinate and act to prevent and respond to such activity. Understanding risks helps Internet users make more informed decisions about their online behavior – whether to open an email from



Credits: iStock.com

an unknown sender, install a verified software update, click on an embedded link, visit an insecure website, or use two factor authentication. Improved user behavior in turn reduces the successfulness of many malicious activities. At the same time, improved software development practices can also reduce vulnerabilities. The combination of these actions, informed through greater transparency, would go a long way to improving security online. And recognizing these improvements would contribute to restoring and increasing trust in the Internet.

In the 2016 *"Cybersecurity, Are We Ready in Latin America and the Caribbean"* report, the Organization of the American States (OAS) and the Inter-American Development Bank highlighted the role of civil society in the developing of public-private part-

nerships to make meaningful cybersecurity advancements. We believe governments should continue the open approach the 2016 report exemplifies as they work to improve cybersecurity at the national and regional levels. A multi-stakeholder approach fosters transparency and ultimately increases awareness because users are better informed about the challenges presented through increasing connectivity and trust the steps taken to address them.

### **Opportunities for transparency and dialogue**

A first and early opportunity governments have to increase transparency and dialogue is in the de-

velopment of national cybersecurity strategies. In this process, which can raise the salience of cybersecurity issues in public debate, governments can and should work with industry and civil society to identify and implement policies to address the identified threats and vulnerabilities.

A transparent and multi-stakeholder approach has various advantages. First, it gives the different stakeholders an opportunity to establish cooperative relations and develop a common understanding of the identified threats and the tools to counter them. Second, it can give all parts greater confidence in the ultimate approach chosen and an understanding of their role in achieving the strategy's objectives. In Latin America, the OAS encourages a multi-stakeholder approach to cybersecurity.

---

## “Immediate steps to enhance internet trust must be taken such as enhanced transparency and the encouragement of multi-stakeholder dialogues”

The development and implementation of best practices for core national cybersecurity activities are also opportunities for transparency and awareness raising. Take for example OAS’ *“Best Practices for Establishing a National Computer Security Incident Response Team”* (CSIRT). The document outlines a CSIRT’s role, offers guidance in the development of the institution’s framework, and identifies core actions the CSIRT should undertake in establishing operations. The best practices include sample policies on use of the CSIRT’s information systems and disclosure of information held by the CSIRT.

Published best practices identify an action a government or other organization should undertake, and the methods through which it should be undertaken. In doing so, best practi-

ces raise awareness of an important cybersecurity activity and establish baselines against which an organization can be evaluated. Best practices can also provide opportunities for accountability of and by governments and civil society.

Public-private partnerships and the transparency they enable also evolve through the development and use of common frameworks, such as the U.S. Department of Commerce National Institute of Standards and Technology “Framework for Improving Critical Infrastructure Cybersecurity,” commonly known as the NIST Framework, and standards such as ISO 27001 “Information Security Management.” NIST developed the Framework through a series of public workshops and feedback sessions. Initially published in 2014, in early 2017 NIST announced it is in the process of updating the Framework, again using requests for public comment, workshops, and webinars to engage stakeholders. In the three years since its publication, 30% of surveyed U.S. companies have adopted the Framework in some form, with the number expected to grow to 50% by 2020. Companies also reported that they use additional frameworks to manage their cybersecurity risk, including ISO 27001/27002.

More recently, in April 2017, the Information Sharing and Analysis Organization Standards Organization requested public comment on draft Guiding Practices to Advance Consumer Privacy in Cybersecurity Information Sharing. Public Knowledge, a

non-profit organization that promotes freedom of expression, an open internet, and access to affordable communications tools and creative works, cooperated with other civil society organizations, the U.S. government, and industry to develop the draft practices, which identify actions that promote user privacy while enabling efficient and effective cybersecurity information sharing. Like the adoption of best practices, organizations that publicize their use of recognized cybersecurity frameworks and standards inform their customers, partners, and relevant governments that they recognize cybersecurity as a risk and are taking responsible measures to address it.

---

## Conclusion

Transparency, multi-stakeholder dialogue, and accountability around cybersecurity risks, capabilities, and activities, are necessary elements for the development of successful cybersecurity policies. In Latin America and the Caribbean, the OAS’ Cybersecurity Capability Maturity Model, the Best Practices for Establishing a National CSIRT, and the NIST Framework are in use and already incorporate some of these elements. Deepening and expanding these elements in cybersecurity policy development is necessary to restore trust online and maintain the internet as an open platform for progress and development.

# Data protection laws and cybersecurity: Challenges for Latin America

---

*Data protection laws and policies are closely related with cybersecurity: either through principles of data security, regulatory powers for secure data handling, or the obligation to notify security incidents to authorities and/or the subjects of personal data. This relation is useful both for enhancing privacy protections and improving the understanding of the cybersecurity threats we are facing. With Europe and the United States working on this issue throughout the last decade, Latin American countries should follow this discourse and address the issue with a view to protect their citizens' rights and improve their cybersecurity capabilities.*

*Written by: Francisco Vera, Protected Data Foundation, Chile*

Nowadays, most of our personal data is stored in a digital platform: our government records, health data, consumer profiles, financial information and our private communications in emails or instant messages can be accessed, altered or copied millions of times, in a matter of milliseconds. The last two years, data breaches like those of Yahoo (→1 billion records), Target (70 million records), ebay (145 million records), Ashley Madison (37 million records) are also possibly happening in Latin America, but this information hardly is not anywhere

to be found. This reality poses a big challenge both for privacy and cybersecurity.

There are several areas where data protection laws and policies are related with cybersecurity. Data protection laws can set general principles of data security and regulatory powers for secure data handling, which requires the adoption of technical measures to ensure that data retains its confidentiality, integrity and availability. On the other side, data protection laws may also contain some provisions obligating data

handlers to notify security incidents to authorities and/or the subjects of that data.

While security measures are necessary to safeguard the privacy of the people who are in fact the data subjects, the obligation to notify security incidents is also essential to improve the cybersecurity of a State. This dimension of security is achieved by aggregating and understanding the type of threats that are evolving in cyberspace, as well as preventing further malicious actions (sometimes involving the use of stolen data, such



Credits: iStock.com

as identity thefts), and preventing future incidents in the same company, industry or the whole country.

In sum, the first step to improve the cybersecurity of a given State is to understand its vulnerabilities, identify the risks it is facing and enhance its capability to analyze the threat landscape. Mandatory incident notification is crucial to gather that information and act on it.

### The situation in Europe and the U.S.

Data protection regulations not only add necessary technical requirements to the data and systems that contain it, but also the requisite measures for managing data in a safe, reliable and confidential manner. While the European Union is moving towards preparing the implementation of its General Data Protection Regulation (GDPR), the United States have a patchwork of regulations that range from

addressing economic sectors in the whole country, to passing data breach laws in most of the States.

The GDPR, adopted in April 2016 and scheduled to enter into force in all EU Member States in May 2018, is an improvement over the Data Protection Directive that dates from 1995 both in terms of substantive provisions and of harmonized implementation. As a Regulation it will be directly applicable to all EU Member States without the need of any implementing national legislation required by Directives. The Regulation establishes responsibilities and duties for those who

---

## “This article explores the challenges in Latin America with Data Protection Laws”

handle personal data, prescribing the adoption of appropriate technical and organizational measures to securely process the information.

The regulation goes even beyond asking the adoption of “appropriate measures”, but provides suggestions of what those security measures could be - like data encryption, ensuring the confidentiality, integrity, availability and resilience of systems coupled with constant assessing of their own measures' effectiveness. On top of that, the Regulation contains clear personal data breach notification rules to the data protection authorities and the data subjects, with sanctions that can go up to the 2% of the annual turnover of a company.

In the United States different federal laws - among others the Health Insurance Portability and Accountability Act of 1996 for health information, the Federal Privacy Act for personal data in the Government's hands, the rules of the Federal Trade Commission with regards to consumers' privacy and personal information - prescribe different security requisites for their respective sectors, or delegate the right to do so. In addition, at State level most States have implemented

laws providing data breach notifications to consumers or authorities.

### Challenges for Latin America

---

Latin American countries while following the European model of having comprehensive data protection regimes, based on principles and rules applicable to all personal data and some special rules for specific types of data, they tend to fall behind European and United States' standards. The main reason for this shortcoming is that most data protection laws were designed following the norms set by the 1995 European Data Protection Directive which was not tailored to address these relatively new issues.

Some countries, like Brazil, don't have a comprehensive data protection law, providing little certainty over the necessary measures that data handlers should adopt to protect personal data, and what are their reporting responsibilities for the notification of security incidents. Other countries, like Argentina or Chile, have outdated laws in this regard, addressing data security only in a generic manner and without specific rules prescribing the notification of security incidents. However, these three countries are in the process of updating their legislative frameworks to address these issues.

Some other countries in the region are more advanced in this area. Among the countries that do have laws addressing data security and notification are Colombia, Mexico,

Peru and Uruguay, but in some cases the only required notification is to the users and not the authority, thereby creating information gaps that affect the gathering of information regarding security incidents which are crucial for cybersecurity purposes.

In addition, having a national cybersecurity strategy is an effective tool to highlight the relation between data protection and cybersecurity. The need to adopt or update data protection legislative frameworks addressing cybersecurity issues is outlined in the cybersecurity strategies of countries like Chile, Colombia, or Paraguay that were published in the last two years.

As the digital economy expands, it is becoming urgent for countries in Latin America to update their data protection legislation to address cybersecurity issues and adopt the necessary technical measures that can safeguard the privacy of data and incorporate effective incident reporting mechanisms. Compared legislation in both Europe and the United States may serve as examples of implementation. Otherwise, Latin American countries will not be capable to protect their citizens' data or gather information that nowadays is essential to develop cybersecurity threat assessments.

# Introducing the Cybersecurity Alliance for Mutual Progress (CAMP)

---

*The purpose of the Cybersecurity Alliance for Mutual Progress (CAMP) is to achieve sustainable benefits of a secure cyber environment and serve as a platform where members take collective action to keep cyberspace safe. Within this network, members will share best practices and analyze current trends in the field of cybersecurity. CAMP believes this will lead to mutual progress and at the same time contribute to the general strengthening of global cybersecurity.*

*Written by: You Jin MOON, Researcher of Korea Internet & Security Agency, also in charge of the CAMP Secretariat*

## Towards a safer tomorrow

---

For a long time, cyberspace has been treated as a purely virtual place, far removed from the physical world. The perception was that cyberattacks were simply perpetrated by hackers, showing off their skills. Today, people's perception of cyberspace has significantly changed. Due to advancements in information technology, the boundaries between cyberspace and the physical world are crumbling even further. Simultaneously, the sophistication of cyberattacks is growing at an alarming pace, and

consequently the resulting threats are more serious. Cyberattacks not only cause socio-economic losses, but are nowadays widely recognized as a threat to national and international security.

Under these circumstances, it is increasingly difficult for a single nation to handle cybersecurity issues on its own. There is a need for stronger and more effective collaboration at the global level, in order to maintain a safe cyberspace. In response to demands from government agencies and public organizations invested in cybersecurity, 37 organizations from 29 different countries gathered to-

gether in 2015 to explore the possibility of forming a new global alliance on cybersecurity. The participants agreed to launch a global initiative. The aim was said to build their cybersecurity capacities and capabilities, and to foster global cooperation in responding to cyber threats. The Joint Statement, adopted at this preparatory gathering, was the starting point of the Cybersecurity Alliance for Mutual Progress (CAMP) and defined its role as a platform to allow member countries and participating organizations to obtain needs-based support and information sharing benefits in the field of cybersecurity, inter alia





Inaugural meeting of the Cybersecurity Alliance for Mutual Progress (CAMP), 11 July 2016, Seoul, South Korea.  
Credits: Korea Internet and Security Agency

on threats prevention and response, privacy and personal data protection, spam prevention, digital identity and public key infrastructure management, Internet of Things (IoT) security, etc.

### The beginning of a global partnership on cybersecurity

CAMP was officially launched on July 11, 2016 in Seoul, Korea with the purpose to achieve sustainable benefits of secure cyber environment and to serve as a platform where

members can take collective action to keep cyberspace safe. As of now, CAMP has 49 member organizations from 37 countries – and this number continues to grow. Government agencies and public and non-profit organizations related to cybersecurity are eligible for CAMP membership.

Thanks to the active participation and contribution of its members, in its first year of operation, CAMP improved and stabilized its organizational structure, continuously shared information on cyber threats, and explored the development of joint cybersecurity projects. The Operations Committee and Working Groups hold regular teleconferences, which serve to promote the organization's ac-

“CAMP’s purpose to achieve sustainable benefits of secure cyber environment and to serve as a platform where members can take collective action to keep cyberspace safe”



Annual meeting. Credits: Korea Internet and Security Agency

tivities and strengthen member relations. CAMP also publishes a monthly newsletter with updates on members' activities and cybersecurity trends.

This year will see the start of CAMP Regional Forums, designed to discuss establishing successful policies and strategies on cybersecurity at the domestic and regional level. The forums also intend to intensify cross-border co-operation and discover potential future tasks for CAMP. The first Regional Forum was held on April 19-20, 2017 in Accra, Ghana. CAMP member representatives and potential members from the African region had in-depth discussions on the current state of cybersecurity in

Africa and shared plans to develop and increase cyber resilience in the region.

Among the most important gatherings for CAMP is the Annual General Meeting (AGM), where all members gather to discuss the direction of operations, exchange experiences and information, and organize activities that advance mutual interests. The second CAMP AGM, carrying the theme of "Cyber Resilience: the Key of Cybersecurity," will be held on July 5, 2017 in Seoul, Korea, and will further build on the progress made thus far.

—

**“CAMP’s purpose to achieve sustainable benefits of secure cyber environment and to serve as a platform where members”**



Technology Exhibition. Credits: Korea Internet and Security Agency

## Building trust for the next generation

As new cyber risks arise and evolve – and new areas of cyber vulnerability emerge – it becomes increasingly harder for countries to manage and respond to cyber threats on their own. Recognizing this reality, CAMP will support close cooperation among its members, with the ultimate goal of forming both a trustworthy and secure cyberspace.

There is a saying that CAMP follows: “Coming together is the beginning. Keeping together is pro-

gress. Working together is success”. The hard work and contribution of all CAMP members will leave a lasting legacy in the field of cybersecurity for the benefit of future generations.

### More information:

Cybersecurity Alliance for Mutual Progress: <https://www.cybersec-alliance.org>

# Singapore's approach to international cyber cooperation

Robust and coordinated capacity building for a secure and resilient cyberspace

---

*To achieve a secure and resilient cyberspace, it is essential for countries to adopt a rules-based system with practical and implementable norms that guide states' behaviour in cyberspace. To this end, Singapore supports robust and coordinated cyber capacity building, and has launched the S\$10 million ASEAN Cyber Capacity Programme (ACCP). The ACCP is a multi-disciplinary, modular, multi-national and multi-stakeholder initiative, and complements existing ASEAN cyber capacity building efforts. Singapore also sponsors the CyberGreen initiative and promotes the ASEAN CERT Maturity Framework, which contribute to capacity building efforts in South East Asia.*

*Written by: Mr. David Koh, Chief Executive, Cyber Security Agency of Singapore (CSA)*

## A rules-based system for cyberspace

---

Cyber is an enabler of economic progress and higher standards of living. As a small state and an international economic hub in areas such as banking and finance, telecommunications, maritime and aviation, Singapore supports a rule-based cyberspace with well-defined practical and implementable voluntary norms of behaviour. As such, Singapore supports the work of the UN Group of

Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, and other international platforms in discussing and developing voluntary norms of behaviour. Singapore stands ready to participate in these conversations and to contribute to them, in partnership with other Member States of the Association of Southeast Asian Nations (ASEAN).

## Singapore's approach to cyber capacity building and its link to confidence building measures

---

For cyberspace to be an effective force for economic progress, it must be governed by well-defined and practical norms of behaviour supported by robust confidence building measures (CBMs). In determining such norms and CBMs, states must be allowed to take into account their unique histo-



ASEAN Ministerial Conference on Cybersecurity (AMCC) 2016. Credits: Cyber Security Agency of Singapore (photo by MCI)

tical and social contexts, and geopolitical situations. When this happens, states can work together to protect their interests in cyberspace in the face of ever-evolving cyber threats.

The ability of individual states to implement these norms and CBMs depends on their domestic cyber capacity, not just in technical and operational areas, e.g. cyber incident response, but also in other areas such as cyber policy and strategy development, drafting of legislation and diplomatic engagement. For individual states to become more confident and secure in cyberspace, they need to enhance their capacities across these different cyber dimensions. Cyber capacity building measures are therefore a key ingredient in national efforts towards increasing their confidence in cyberspace, as well as in enhancing the security and resilience of the broader cyber ecosystem. In

this regard, Singapore welcomes initiatives such as those spearheaded by the Global Forum for Cyber Expertise (GFCE) to coordinate and enhance global cyber capacity building actions.

### Singapore's ASEAN Cyber Capacity Programme (ACCP)

To highlight the importance of cyber capacity building, Singapore's Minister-in-charge of Cybersecurity Dr. Yaacob Ibrahim announced during the inaugural Singapore International Cyber Week (SICW) in October 2016 the launch of the S\$10 million ASEAN Cyber Capacity Programme (ACCP). The ACCP complements existing ASEAN cyber capacity building efforts, and has five key features:

- **Multi-disciplinary**

It covers not only technical and operational areas, but also strategic and legislative areas, including cyber policy, strategy, and legislation building as well as cyber diplomacy.

- **Modular and flexible:**

This will allow programmes to be tailored to the needs of different stakeholders, ensuring a targeted approach to capacity building.

- **Multi-national coordination:**

It is more effective for countries to pool resources for international and regional cyber capacity building efforts. This coordination avoids overlap and duplication of efforts. Since 2016, Singapore has started cooperating with trainers from the United States, the Netherlands, the United Kingdom, Japan and Australia as well as the various ASEAN Member States

## “Cyber capacity building measures are a key ingredient towards increasing confidence in cyberspace as well as enhancing the security and resilience of the cyber ecosystem”

in capacity building efforts.

- **Multi-stakeholder:**

Singapore recognises the expertise and resources that industry, NGOs and academia can bring to cyber capacity building. The ACCP will involve these stakeholders to enhance the quality and breadth of our programmes.

- **Complementary:**

ACCP seeks to work with existing international and regional cyber capacity initiatives, including the CyberGreen initiative, so as to minimize duplication and to benefit from a well-coordinated effort.

Within the ACCP, Singapore plans to organize regular ASEAN Cyber Norms and ASEAN Cybersecurity Capacity Building workshops, in collaboration with the Singapore Cooperation Programme and Third Country

Training Programme. As part of our contribution to continuing ASEAN and international cybersecurity discussions, Singapore will host the second Singapore International Cyber Week (SICW) from 18-21 September 2017. During the same week, Singapore will also host the second ASEAN Ministerial Conference on Cybersecurity (AMCC) and the International Cyber Leaders' Symposium (ICLS).

### Supporting regional cyber capacity building in ASEAN

Singapore promotes the ASEAN CERT maturity framework, which enhances ASEAN's approach to levelling up incident response capabilities in a coordinated and targeted manner. It can serve as a common reference to determine the maturity level of respective ASEAN Member States' national CERTs, and systematically identify gap areas to which appropriate training or capacity building effort can be directed. A common framework will also enable mutual understanding and facilitate enhanced collaboration among CERT partners in times of need, thereby increasing the collective cybersecurity level of ASEAN. ASEAN can further bolster its cyber capacity through the ASEAN CERT Maturity Framework, in collaboration with Dialogue Partners and international organisations, in areas such as information sharing, threat awareness building, exchange of best practices, CERT-CERT cooperation and exercises. These build on existing efforts, like the ASEAN CERT Incident Drill (ACID), which Singapore has been hosting since 2006.

Moreover, Singapore is a key sponsor of CyberGreen, a global initiative to create a resilient and healthy cyber ecosystem. CyberGreen has a well-established system to aggregate global open source information into an index for cyber health, which is, amongst others, available for ASEAN Member States to assess their own cyber health status. The increased awareness is aimed at empowering ASEAN Member States to take appropriate preventive actions and to better mitigate cyber threats. The Singapore Computer Emergency Response Team (SingCERT), under the Cyber Security Agency of Singapore (CSA), will collaborate with CyberGreen to identify different levels of threats and develop response mechanisms required to counter these threats.

All in all, Singapore's underlying approach to cyber cooperation is grounded in a rules-based system for cyberspace – one that is secure, resilient and strengthened by comprehensive and coordinated capacity building. Together with the agreement on international cyber norms guiding states' behaviour in cyberspace and the development of confidence building measures, they form a holistic model of international cyber engagement.

#### More information:

Announcement of the ASEAN Cyber Capacity Programme (ACCP):  
[https://www.csa.gov.sg/-/media/csa/documents/amcc%20factsheet/factsheet\\_accp.pdf?la=en](https://www.csa.gov.sg/-/media/csa/documents/amcc%20factsheet/factsheet_accp.pdf?la=en)

CyberGreen:  
<http://www.cybergreen.net/>

# The EU's efforts in fighting cybercrime:

Putting together legislative action, cross-sectoral and international cooperation, as well as capacity building

---

*Cybercrime has evolved into one of the greatest challenges for the rule of law across criminal jurisdictions while the penetration of electronic evidence into of any type of crime further complicates the puzzle for criminal justice authorities. The EU's approach the fight against cybercrime consists of a comprehensive toolkit that involves the adoption and update of appropriate legislation; the support to cooperation frameworks amongst criminal justice actors and across sectors particularly with industry; and increased focus on research and development as well as training programmes that provide access to the right technology and enhance the capacities and expertise of law enforcement and judiciary.*

*Written by: Michele Socco, Policy Officer, Cybercrime Unit, Directorate General for Migration and Home Affairs, European Commission.*

## Crime in the era of new technologies

---

As the digital dimension of our lives is increasing, so is the criminal activity in the cyber environment. The borderless nature of cybercrime, coupled with its characteristic low risk-high reward business model, has contributed to the wide-spreading of criminal activities where computers and information systems are involved either as a primary tool or as a primary target. The cyber

dimension in most types of crimes has been constantly on the rise in the last decade, with the cross-over of the use of new technologies by organised crime groups is no longer an alarming trend but a reality. Criminals quickly deploy and adapt new technologies into their *modi operandi* or build brand-new business models around them with great skill and to great effect.

Fighting cybercrime more effectively is one of the three priorities under the European Agenda on Security that was adopted in April 2015, while

it is also a basic pillar of the EU's 2013 Cybersecurity Strategy that is currently under revision. Also within the framework of the multi-annual EU Policy Cycle for Serious and Organised Crime that ensures effective cooperation and coherent operational action targeting the most pressing criminal threats facing the EU, cybercrime is one of the priority areas of EMPACT (European multidisciplinary platform against criminal threats) that translates the Policy Cycle's strategic objectives into concrete operational actions.

“Criminals quickly deploy and adapt new technologies into their modus operandi or build brand-new business models around them with great skill and to great effect.”



European Cybercrime Centre (EC3), Multi-Disciplinary Centre for Cyber Innovation (MDCCI). Credits: Europol

The EU's approach to the fight against cybercrime consists of a comprehensive set of actions along three main focal areas: appropriate legal framework; cooperation frameworks amongst criminal justice actors and across sectors particularly with industry which controls a large part of information infrastructures; and financial resources to allow for research and development that provide access to the right technology to address market failures, as well as training programmes to enhance the capacities and expertise of law enforcement and judiciary in this area.

## Legislative action as the foundation

Specifically on the legislative front, the key measures for the EU's cybercrime framework include:

- The **2013 Directive on attacks against information systems**

which aims to tackle large-scale cyber attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions.

- The **2011 Directive on combating the sexual exploitation of children online and child pornography**, which better addresses new developments in the online environment, such as grooming.
- The **2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payment**, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences. The European Commission is currently working towards the revision of this Framework Decision to cover new forms of money transmissions like virtual currencies and other aspects.

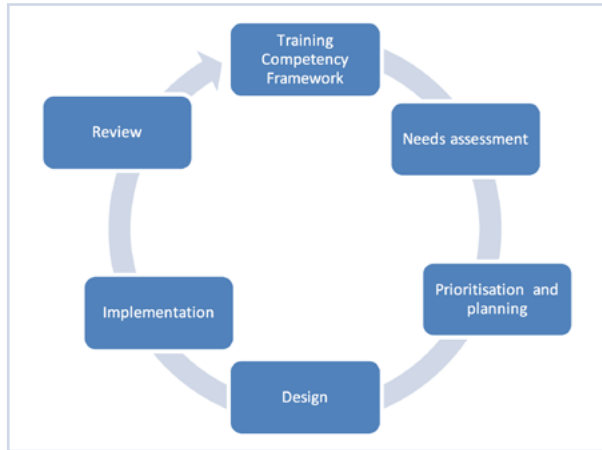
These legislative measures are

based on existing standards and the models that capture international best practice frameworks of reference, namely the Council of Europe 'Budapest Convention on Cybercrime' and the 'Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse'.

Complementary to these are related legislative initiatives, such as the 2016 Directive on Network and Information Security and the 2002 e-Privacy Directive which is currently under revision to align to the requirements of the General Data Protection Regulation of 2016, while a new strand of work is currently undertaken on the need to improve the enforcement of the rule of law in cyberspace and obtaining electronic evidence in criminal proceedings, including cross-border access to e-evidence.

Nevertheless, legislation is only the foundation for an effective response to cybercrime which needs to be coupled with the necessary skills to prevent, detect, prosecute and adjudicate cybercrime as well as with operational international cooperation.





Key steps addressed by the Training Governance Model, CEPOL

and provide up to date training. Each stakeholder has a role in the different steps of the TGM.

As part of the TGM, the creation of a Training Competency Framework (TCF) on Cybercrime serves as the basis for identification of the required competencies and skills in combating cybercrime for key actors ranging from law enforcement to the judiciary. As the area of cybercrime is extremely dynamic, the TCF is periodically reviewed and updated when necessary. The EU-wide needs assessment is also fundamental in identifying gaps of existing skillset and training repositories of the law enforcement and the judiciary that feeds into the prioritisation exercise. For the training design and development, EC-TEG is in the lead as its objective is to provide experience and knowledge to further enhance the coordination of cybercrime training through the development of a robust and enduring training programme. Within the TGM, delivery of training is mainly led by CEPOL and the European Judicial Training Network (EJTN) that are generally responsible for the implementation of training and learning activities at European level.

Complimentary actions to creating the necessary knowledge entail research and innovation projects on digital forensics, enhancing cybersecurity and prevention, analysis of large set of data that the EU has financed through its research programme, Horizon 2020. In an effort to ensure that research is indeed targeted to the needs of law enforcement, the EU has also financed the creation of Cybercrime Centres of Excellence (in 15 EU countries) that foster the partnership between private companies, academia and law enforcement.

While these measures are functional to develop capacity within the EU, considering the borderless nature of cybercrime the EU is very much committed and engaged to capacity building in partner countries as well.

## Operational cooperation across sectors and countries

Some key cooperation mechanisms and structures the EU has set up has been the European Cybercrime Centre at Europol (EC3) which since 2013 serves as a central hub for criminal information and intelligence and supports operations and investigations by EU Member States by offering operational analysis, coordination and technical expertise. It also provides a variety of strategic-analysis products, such as the Internet Organised Crime Threat Assessment, while it applies a comprehensive outreach function with other international partners such as INTERPOL and connects with the private sector, academia and other non-law enforcement partners. In the few years since its establishment, EC3 has already made a significant contribution to the fight against cybercrime: the number of high profile operations it supported steadily grew from 57 in 2013 to 175 in 2016. Two other significant steps in enhanced cooperation include the establishment of the EU Internet Forum in 2015 with the aim to reach a joint, voluntary approach based on a public-private partnership with ISPs to detect and address harmful material online; as well as the creation

of the European Judicial Cybercrime Network in 2016 to facilitate sharing expertise, knowledge and best practice amongst experts from competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace.

## Bridging the skills' gap

Moreover, there is broad consensus between practitioners and researchers that cybercrime investigations are hindered by insufficient knowledge and a skill gap of law enforcement officers as well as the relevant actors in the judiciary. In order to meet the vast needs of stakeholders in a concerted, complementary and sustainable manner, the key EU stakeholders - namely the European Commission, EC3 at Europol, the European Cybercrime Training and Education Group (ECTEG), the EU Agency for Law Enforcement Training (CEPOL) and Eurojust - agreed in 2015 to develop a Training Governance Model (TGM) on cybercrime. The TGM is intended to enable the creation of an effective, well-established, coordinated and sustainable mechanism that can meet the operational challenges and needs,

# Cybersecurity in Ukraine: National Strategy and international cooperation

---

*In response to large-scale attacks to its critical infrastructure in recent years, Ukraine adopted in 2016 a National Cybersecurity Strategy and is making strides in its implementation. The set up of the National Cybersecurity Coordination Center in 2016 and the proposed update of the cybercrime legislation to meet the Budapest Convention requirements and best practice particularly on Internet Service Providers are two main steps in enhancing the country's cyber resilience. These activities are complimented by strong cooperation with international partners across the cyber sphere, including on cybercrime, cybercrime and cyber defence.*

*Written by: Oleksii Tkachenko, International Relations Officer,  
Cyber Department, Security Service of Ukraine*

## A complex cyber threat landscape

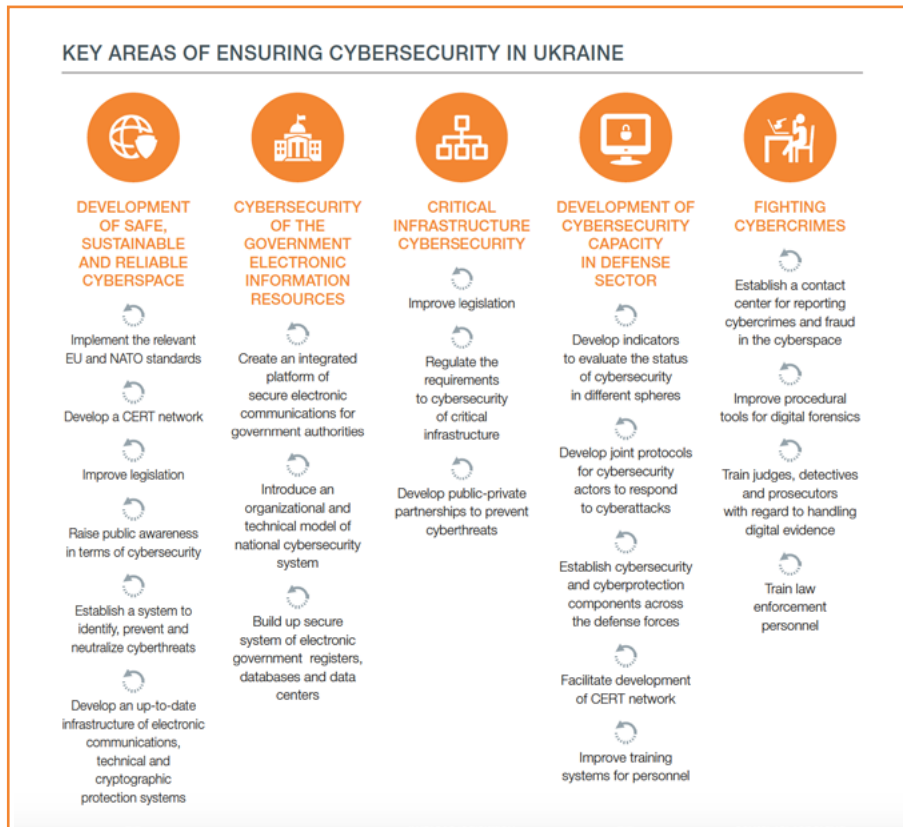
---

Increased digitalization of services and reliance to the internet have brought about the evolution of cyberspace, raising also significant security challenges to governments across the globe vis-à-vis offences against and by means of computer systems. In Ukraine this has been demonstrated most significantly with the large-scale cyber attacks to Ukrainian power com-

panies in December 2015 following attacks to major Ukrainian TV channels two months earlier on the day of local elections.

These incidents fit within the overall trend that Ukraine is witnessing the past years with an increased use of Distributed Denial of Service attacks as well as zero-day vulnerabilities exploited to penetrate and compromise critical infrastructures. The threat landscape analysis also points to targeted attacks on diplomats, law enforcement agencies, defense actors, sta-

te enterprises, mass media, as well as politicians and public figures, as well as misinformation campaigns over the Internet to influence the 'physical' world. The impact of these attacks can be significant as they can damage critical infrastructures and hinder the effective functioning of the national authorities. Information and psychological warfare aims at discrediting state power and fosters the conditions for the destabilization of the social and political situation.



Source: National Cybersecurity Strategy of Ukraine. Credits for the graph: StratComUA.

## Adoption of the National Cybersecurity Strategy

In response to these challenges, Ukraine adopted by Presidential decree its National Cybersecurity Strategy on 15 February 2016. The Strategy, which is coupled with an annual Action Plan for its implementation, has as an overarching goal to create the conditions that ensure safe cyberspace and its use in the interests of individuals, the society and the Government. The main focus of the Strategy is on three axes:

- Developing the national cybersecurity system
- Enhancing capabilities across the security and defence sector
- Ensuring the cybersecurity of critical information infrastructure and of Government information resources.

The national cybersecurity system put in place by the Strategy ensures collaboration between all government agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civil groups, businesses, and organizations, irrespective of their form

“The National Cybersecurity Strategy has as an overarching goal to create the conditions that ensure safe cyberspace and its use in the interests of individuals, the society and the Government”

of ownership, that deal with electronic communications and information security or are owners of critical information infrastructure.

A key step in the implementation of the Strategy has been the establishment of the National Cybersecurity Coordination Center in June 2016, which is a working body of the National Security and Defense Council. The Center has a supervising function and undertakes tasks related to analyzing the state of national cybersecurity and its preparedness for combating cyber threats, as well as forecasting and detecting relevant potential and actual threats. It will also participate in

organizing and holding international and interdepartmental cybersecurity training courses.

Moreover, as a State Party to the Budapest Convention on Cybercrime, Ukraine is working towards full implementation of the Convention. Draft legislation has been prepared and is currently discussed in Parliament which entails the strengthening of the liability for cybercrimes, and defines the important terminology and update of responsibilities of the Internet Service Providers (ISPs) according to the Convention.

## International Cooperation and Capacity Building

In recognizing the need for strong international cooperation and capacity building to address cybersecurity needs and threats that is also highlighted in the new Strategy, Ukraine has been collaborating with a number of partners across the cyber domain.

In the area of cybercrime, Ukraine has been a partner in the joint European Union and Council of Europe projects 'CyberCrime@EaP II' and 'CyberCrime@EaP III' that have a regional dimension involving all countries of the Eastern Partnership (i.e. Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine). The first

project is focused on improving mutual legal assistance for international cooperation on cybercrime and electronic evidence and on strengthening the role of 24/7 contact points. The second project, which was launched in Kiev in April 2016, is tackling issues of public and private cooperation. The engagement with the ISPs and the Council of Europe recommendations are already benefitting the national authorities as they have fostered a structured dialogue with ISPs that has served as a trust-building exercise towards understanding and responding to each other's needs. In addition, British and Estonian partners have provided modern hardware and software to Ukrainian law enforcement agencies that to conduct professional computer forensics and investigate cybercrimes more thoroughly.

In the cyber defense field, Ukraine is working with the NATO Cyber Defence Trust Fund to enhance the country's technical capabilities in counter cyber threats. Assistance includes establishing an Incident Management Centre to monitor cyber security events, as well as laboratories to investigate cyber security incidents, coupled with training in employing this technology and equipment. The Security Service of Ukraine is taking the lead role in the framework of the Trust Fund, while the NATO partners include Romania as the lead nation with additional financial and in-kind

contributions from Albania, Estonia, Hungary, Italy, Portugal, Turkey, and the United States. Together with the NATO partners, Ukraine has conducted cyber defense exercises and trainings where all the relevant national stakeholders are trained on how react to major cyber attacks at the national defense infrastructure.

Ukraine is not only participating in the international initiatives in the sphere of countering cyber threats but also contributing to the development of regional initiatives. With an initiative led by Ukraine, a working group on cybersecurity was established in the framework of the GUAM Organization for Democracy and Economic Development (i.e. Azerbaijan, Georgia, Moldova, Ukraine). The group is now discussing the development of a Memorandum of Understanding for adoption by its governments, while it has already put in place a protected communication system which allows, inter alia, the secure exchange data online and conducting of video conferences.

The Ukrainian experience demonstrates that in order to address serious and persistent cyber threats and attacks there is a need for enhanced collaboration at multiple levels - amongst national authorities, with the private sector and with international partners in order to build the necessary capacities and respond effectively to such threats.

# A trusted cyber foundation for the Fourth Industrial Revolution

---

*Human race has always advanced with every twist of our technological evolution. Modern society is increasingly dependent on a mix of core technological breakthroughs. Numerous devices and networks are vital to our daily professional and personal lives and have catalyzed transformations in business, politics, and society. At the same time, cyber threats – including the theft of intellectual property, critical infrastructure attacks, espionage, and war played over the cyber domain – concern everyone, from the White House situation room, to Fortune 500 board rooms, to our living rooms where cyber breaches make headlines daily.*

*Written by: Danil Kerimi, Head, Technology Industries, World Economic Forum; Member of the Advisory Board to the Stanford Cyber Policy Program, Center for International Security and Cooperation/Hoover Institution.*

## Fourth Industrial Revolution

---

Today we live in an enormously complex and hyper-connected world. It brings us both unprecedented opportunities and risks that were unimaginable just few years ago. We are just now starting to understand social, political and economic changes that are brought by adjusting norms, policies and business models to the metaphysics of the network.

This complexity is caused by the

Fourth Industrial Revolution that is quickly erasing boundaries of physical, digital, and biological ecosystems.

### Shift in the collective mind-set

---

To navigate this revolution successfully we need to adopt a systemic view, focusing on the society and striving for inclusiveness. For that we need to ensure that human values are at the core for the development rather





than treat them as a bug to be addressed down the road.

Public authorities today can be overwhelmed by the speed of technological change and the scope of its intended and unintended implications. Many of the technological breakthroughs are scarcely addressed by the current regulatory frameworks. In many cases this is done on purpose, in others by omission. Yet, in most of the developing world this trend persists due to the lack of the capacity, while, when this issue is dealt with, it is often done only with a protective mind-set

“The Fourth Industrial Revolution is quickly erasing boundaries of physical, digital, and biological ecosystems”

### Navigating the next industrial revolution



Revolution	Year	What happened?
	1 1784	Steam, water, mechanical production equipment
	2 1870	Division of labour, electricity, mass production
	3 1969	The computer, electronics and the internet
	4 ?	The barriers between man and machine dissolve



World Economic Forum's Center for the Fourth Industrial Revolution in San Francisco, United States. Credits: World Economic Forum

which often excludes the potential benefits of technology. Regulators and policymakers must find ways to continuously adapt to a new, fast-changing environment by building up their own capacities to thoroughly understand the complex areas they are regulating. It is therefore critical that the public and private sector comprehend the technological evolution and are ready to

create policies that are as innovative as the change that is happening.

### Center for the Fourth Industrial Revolution

To advance this objective, the World Economic Forum has opened

its new [Center for the Fourth Industrial Revolution in San Francisco](#). Leveraging the Forum's multistakeholder platform, the Center is committed to advance the technology governance for the benefit of society.

Given the accelerating change brought on by innovation, continuous public-private cooperation on a global level is needed more than ever. The

purpose of the Center is to contribute to this end and serve as a global platform for dialogue and collaborative action on the most important questions related to the impact of emerging technologies.

Among its early projects, the Center will facilitate the development of the [Digital Protocol Networks](#) – tools for the global community to address complex transnational issues affecting the digital society. Three early pilots that aim to deliver non-binding policy frameworks have already started their work:

- **The National Digital Policies Network** enables the development of national and transnational digital policy structures through addressing the various elements of national digital strategy;
- **The Industrial Internet of Things (IoT) Safety Network** looks at any potential market failure that would reduce the trust in IoT. It will do so by developing a set of criteria for what constitutes a “safe” IoT endpoints and by evaluation current security frameworks as well as incentives for all actors.
- **The Artificial Intelligence (AI) and Future of Trust Network** increases awareness among senior leaders on the need for framing the emerging and probable societal risks of artificial intelligence.

All these efforts are undertaken with all our partners from business, government and civil society and aim to complement other efforts that are already taking place.

## Stanford Cyber Policy Program

One such effort, that is particularly relevant for cyber capacity building is the [Stanford Cyber Policy Program](#) co-created by the Hoover Institution and the Center for International Security and Cooperation at Stanford University in 2015. The program’s mission is to solve the most important international cyber policy challenges by conducting world class policy-driven research across disciplines, serving as a trusted convener across sectors and teaching the next generation of cyber leaders.

The landscape of important cyber policy questions is vast, ranging from how to secure nuclear power plants, to maintaining consumer trust in the financial sector, to understanding and managing escalation dynamics in cyber conflicts. The Program focuses principally on issues requiring an interdisciplinary approach and is fit for purpose to several key audiences:

- **For policymakers:** it seeks to provide in-depth expertise through papers, briefings, access to the latest research, and events.
- **For the private sector:** it provides an efficient, effective, and trusted platform for engaging with policy makers to express and share concerns related to cyber policy and security.
- **For civil society:** the program is poised to play an important role in establishing and building cyber policy as an area of research

---

“The future of digital economy will be built on the strong cyber foundation rooted in confidence, reliability and security”

specialization and a potential training ground for future thought leaders.

## Trust in the digital world

The future of digital economy will be built on the strong cyber foundation rooted in confidence, reliability and security. Despite an increasing level of awareness, the adoption of national digital and cyber strategies is still divergent as technology continues to disrupt industries, governments and societies. Innovation and technology can become a foundation of the economic competitiveness if societies address capacity building in the most comprehensive way possible. The efforts of the GFCE are most needed and timely to ensure that the trust in cyberspace is restored.

# Interview: Alexander Klimburg on the Global Commission on the Stability of Cyberspace



Alexander Klimburg. Credits: HCSS

---

**“A major challenge is the insufficient awareness and mutual acceptance of various cyberspace communities working on issues related to international security in and of cyberspace.”**

The Global Commission on the Stability of Cyberspace (GCSC) is helping to promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. By finding

ways to link the dialogues on international security with the new communities created by cyberspace, the GCSC has a genuine opportunity to contribute to an essential global task: supporting policy and norms coherence related

to the security and stability in and of cyberspace. Alexander Klimburg (Hague Centre for Strategic Studies) is co-director of the GCSC Secretariat together with Bruce McConnell (East West Institute).





Alexander Klimburg, Minister Bert Koenders, GCSC Chair Marina Kaljurand, Co-Chairs Latha Reddy and Michael Chertoff, and Commissioner Prof Joseph Nye (from left to right) at the launch of the GCSC at the 2017 Munich Security Conference.



**GLOBAL COMMISSION**  
ON THE STABILITY OF CYBERSPACE

### Q: Why was the Global Commission on the Stability of Cyberspace established?

The overall motives for the establishment of the Global Commission on the Stability of Cyberspace (GCSC) include the complex governance and security architecture making it difficult to reach durable norms and policies that are supported by all stakeholders, and the increase of offensive cyber operations that risk undermining the peaceful use of cyberspace to facilitate economic growth and the expansion of individual freedoms.

Additionally, a major challenge is the insufficient awareness and mutual acceptance of various cyberspace communities working on issues related to international security in and of cyberspace.

As expressed in the 2015 consensus report of the UN Group of Governmental Experts (UNGGE) on Develop-

ments in the Field of Information and Telecommunications in the Context of International Security:

“While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations”<sup>[1]</sup>

By finding ways to link the well-established dialogues on international security with new cyberspace communities, the GCSC has a genuine opportunity to support policy coherence related to the security and stability in and of cyberspace.

### Q: What are the core objectives of the GCSC and how does it operate?

The GCSC will develop proposals for norms and policies to enhance international security and stability and

guide responsible state and non-state behavior in cyberspace. The GCSC will engage the full range of stakeholders to develop shared understandings, and its work will advance cyber stability by supporting information exchange and capacity building, basic research, and advocacy.

[Our Commissioners](#) set the research agenda. In February, we had our (small) Inaugural meeting after our launch at the Munich Security Conference. Many interesting and vital topics were raised, and by this summer, we hope to agree on the first topic for research.

Our information exchange will take many forms. We will physically meet a number of times over a three year period, encouraging the flow of information and knowledge across various cyberspace initiatives, as well as cross-fertilization and capacity building. For our full Commission Meetings, government and academic

“Cyber capacity building will most likely play an increasingly important role in future foreign policy considerations. It is essential in connecting the economic, international security, and human rights, and development discourses.”

experts will be able to join in order to ensure the GCSC remains relevant to the developments in these processes.

We are starting recruitment for our Research Advisory Group soon. Together with this research group, the Commission will fund and conduct research on norms, as well as on emerging themes and ideas of relevance to the stability of cyberspace.

Finally, the Commission will formulate recommendations for action, applicable to both state and non-state led initiatives. The Commission will advocate for these recommendations in capitals, corporate headquarters, and civil society centers, as well as the wider public.

Drawing on the work of previous commissions and the London Process, the GCSC will thus bring toge-

ther thought leaders, researchers, and practitioners from the world of international cybersecurity, Internet governance, technical and information practices, and the legal domain into a wider dialogue towards a better understanding of the interactions of the diverse regimes.

If you want to remain involved in the developments of the GCSC, please visit <https://cyberstability.org/> or follow us on twitter [@theGCSC](https://twitter.com/theGCSC)

**Q: What is the vision of the GCSC on the importance of Cyber Capacity Building?**

In order to promote and enhance stability, Cyber Capacity Building is a necessary element. It is a means to enhance the overall level of cybersecurity, bridge the digital gap and build up mutual trust. It is an important step for cooperation and confidence building.

Cyber capacity building will most likely play an increasingly important role in future foreign policy considerations. It is essential in connecting the economic, international security, and human rights, and development discourses. More specifically, it is becoming increasingly clear that access to cyber space is a key factor in economic and social development, and as such political stability). In turn, cyber security becomes a key ingredient for ensuring access is not jeopardized through predatory criminal or malign behavior.

Moreover, given the nature of the Internet, increased cooperation between the industrialized and the developing world is needed to be able to respond to cyber-threats. Such cooperation can be possible only if basic cyber security institutions and

skills are present in the partner countries – which is very much in the direct interest of donor countries.

**Q: Are there ways how the GCSC and the GFCE can support or complement each other towards the goal of a more resilient and secure cyberspace?**

The word *capacity building* is specifically mentioned as one of the primary goals of the GCSC as part of *information exchange*. We particularly see it as necessary for specific individuals in the global south and also its importance for raising awareness for experts working in particular silos. In effect, we believe capacity building will promote mutual awareness, across both technical specialty areas and regional boundaries.

We are therefore following the work of the GFCE with keen interest. Not only is the operational work of vital importance – raising cybersecurity standards are seen as playing a crucial role for international peace and security in cyberspace – but also the ability of actors in the developing world to engage in these discussions.

Both the GCSC and GFCE should examine how we could potentially mutually enforce our efforts in this regard.

**More information:**

[1] UNGGE 2015 Report, paragraph 31 on p.13, available at [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174)

# Working towards a global cyber capacity building agenda in 2017

Over the past years there has been an increasing interest in the topic of cyber capacity building within the international community. This was highlighted during the third 'London Process'[1] conference in Seoul in 2013, where cyber capacity building was put high on the agenda. During the fourth conference, the Global Conference on CyberSpace (GCCS) in The Hague, the Netherlands, a structure was provided for global cyber capacity building. The Global Forum on Cyber Expertise (GFCE) was launched as a concrete deliverable of this conference with the aim to serve as a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. In less than two years, the number of GFCE Members and GFCE initiatives has expanded beyond expectations. With the prospect of the fifth GCCS conference taking place in November 2017, the next steps include efforts towards defining a shared global agenda on cyber capacity building.

Written by: Manon van Tienhoven and the GFCE Advisory Board

## A Global Agenda on cyber capacity building

The **global agenda** on cyber capacity building is intended to be a shared agenda with an agreed ambition on the priority setting of cyber capacity building topics; for example, a cybersecurity strategy for every

country or a substantial increase of the number of CERTs worldwide. In collaboration with its Members, Partners and Advisory Board, the GFCE will then steer the development of an internationally coordinated response to meet these cyber capacity building priorities.

## Identifying global good practices

The GFCE can help to identify **global good practices** based on the information collected from GFCE initiatives' experiences and expertise. Good practices are not intended as a 'one-size-fits-all' model. Rather, the-



Ministry of Electronics & Information  
Technology  
Government of India

Official handover of the Global Conference on CyberSpace from the Ambassador of the Netherlands, Alphonsus Stoelinga, to the Indian Minister of IT and Law, Ravi Shankar Prasad. Credits (GCCS India): Electronic Media

se are supposed to be recommendations systematized in a practical document (e.g. toolkit or guidelines) as to how stakeholders can implement and strengthen their cyber capacity building efforts. Other sources for the global good practices are the broader experiences of the GFCE community and other widely recognized sources such as those developed by regional and international organizations.

Members and initiatives, proving that it is an effective forum to facilitate the international multistakeholders' need for cooperation and coordination on cyber capacity building. The GCCS 2017 in India will be the next milestone for the GFCE, where it can present itself as a worldwide platform and to give a political impulse to the importance of cyber capacity building. In 2018 the GFCE

endeavors to shift the focus from awareness of cyber capacity building on a global level towards increased and improved implementation. The realization of the global agenda and the GFCE global good practices will be the two pillars which will be crucial in determining on how and on which topics the GFCE community will move towards implementation.

## Looking ahead

The overall objective is to make 2017 a turning point for a new phase in cyber capacity building which will accelerate developments by merging the best GFCE-related cyber efforts with experience and expertise from capacity development communities worldwide. The GFCE has evolved since its launch in 2015 with a significant increase in

### Introducing GFCE co-chair Ms. Aruna Sundararajan as the representative for India

Ms. Aruna Sundararajan is an IAS officer of 1982 batch, Kerala Cadre. In her current role as Secretary, Ministry of Electronics & Information Technology, Government of India, Ms. Sundararajan leads policy making at the highest level in achieving the Ministry's vision and mission as the engine for India's transformation into an inclusive and empowered digital economy.



Installation of the GFCE Advisory Board during the GFCE Annual Meeting 2016 in Washington DC.

“With the prospect of the fifth GCCS conference taking place in November 2017, the next steps are taken on the topic with the aim to reach a shared global agenda on cyber capacity building.”

### GFCE Advisory Board: a year later

The mission of the AB is to provide ‘nonbinding but formal guidance to the GFCE Members on cyber capacity building’, as well as to advise on GFCE initiatives and propose its own, as well as to engage in outreach. The AB Members have spent their initial months of their two-year term on tasks necessary for establishing a productive and sustainable working relationship of the AB. The initial Terms of Reference have been revised, adapting them to the Members’ best understanding of their mandate and its implementation; and Rules of Procedure were adopted to suit the AB modus operandi. Current efforts are focusing on prioritizing strategic goals within an Action Plan for the remainder of the AB’s inaugural term. So far, the AB has provided input into the GFCE Strategy and Roadmap documents. Outreach to Members and Partners in order to further the GFCE goals and initiatives is a high priority: AB members serve at the behest of the GFCE Members, and are committed to supporting Members’ capacity building actions.

The AB welcomes any comments, questions and ideas – it is easy to be in touch via the GFCE Secretariat at [contact@thegfce.com](mailto:contact@thegfce.com)

#### More information:

[1] The London Process refers to a series of international cyber conferences, whereof the first conference took place in 2011 in London.



## Colophon

<b>Editorial board</b>	Manon van Tienhoven (GFCE) Belisario Contreras (OAS) Panagiota-Nayia Barmpalou (EU) Souhila Amazouz (AU)
<b>Guest editors</b>	Dawit Bekele Ilias Chantzos Danil Kermi David Koh You Jin Moon Agustin 'Gus' Rossi Michele Socco Megan Stifel Oleksii Tkachenko Francisco Vera Moctar Yedaly
<b>Artwork &amp; design</b>	Ivonne Vivanco (OAS)
<b>Chief editor (rotating)</b>	Panagiota-Nayia Barmpalou (EU)

---

## Publishers

**African Union**, [www.au.int](http://www.au.int),  
[contact@africa-union.org](mailto:contact@africa-union.org), [@\\_AfricanUnion](https://twitter.com/_AfricanUnion)

**European Union**, [www.europa.eu](http://www.europa.eu),  
[SECPOL-3@eeas.europa.eu](mailto:SECPOL-3@eeas.europa.eu), [@EU\\_Commission](https://twitter.com/EU_Commission)

**Global Forum on Cyber Expertise**, [www.thegfce.com](http://www.thegfce.com),  
[contact@thegfce.com](mailto:contact@thegfce.com), [@thegfce](https://twitter.com/thegfce)

**Organization of American States**, [www.oas.org/cyber](http://www.oas.org/cyber),  
[cybersecutiry@oas.org](mailto:cybersecutiry@oas.org), [@OEA\\_Cyber](https://twitter.com/OEA_Cyber)

---

## Disclaimer

The opinions expressed in this publication are solely those of the authors and do not necessarily reflect the views of the AU, EU, GFCE or OAS or the countries they comprise of.

# CYBERSECURITY CAPACITY PORTAL

## A Global Resource for Cybersecurity Capacity Building

The publically-available online platform of the Global Cyber Security Capacity Centre is designed to be a central point of reference to those responsible for cybersecurity capacity building across the world. It provides up-to-date curated content on new developments and good practices in capacity building. It also includes — in partnership with the GFCE — an inventory of current international and regional capacity-building programmes and projects around the world that may be leveraged to expedite the impact and efficiency of cybersecurity capacity building.

Visit: [www.sbs.ox.ac.uk/cybersecurity-capacity](http://www.sbs.ox.ac.uk/cybersecurity-capacity)



Global  
Cyber Security  
Capacity Centre



For more information: [cybercapacity@oxfordmartin.ox.ac.uk](mailto:cybercapacity@oxfordmartin.ox.ac.uk) | [www.oxfordmartin.ox.ac.uk/cybersecurity](http://www.oxfordmartin.ox.ac.uk/cybersecurity)

Global Cyber Expertise Magazine  
AU | EU | GFCE | OAS  
[contact@thegfce.com](mailto:contact@thegfce.com)

---

Deadline submissions issue 4:  
September 29<sup>th</sup>, 2017