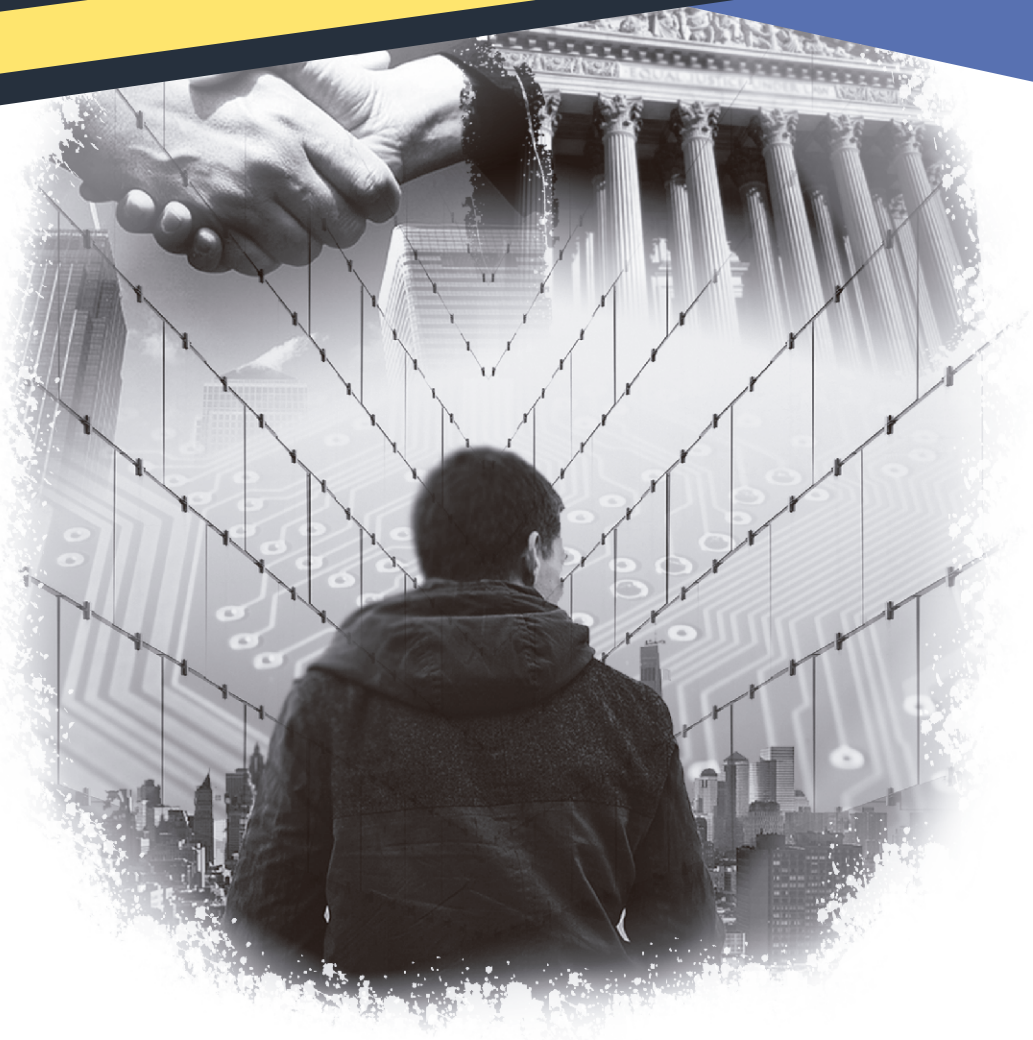
2018

White paper series
Issue 1

A CALL TO ACTION

TO PROTECT CITIZENS THE PRIVATE SECTOR AND GOVERNMENTS



OAS More rights for more people

aws

CREDITS

Luis Almagro

Secretary General of the
Organization of American
States (OAS)

Principal Author

Miguel Rego

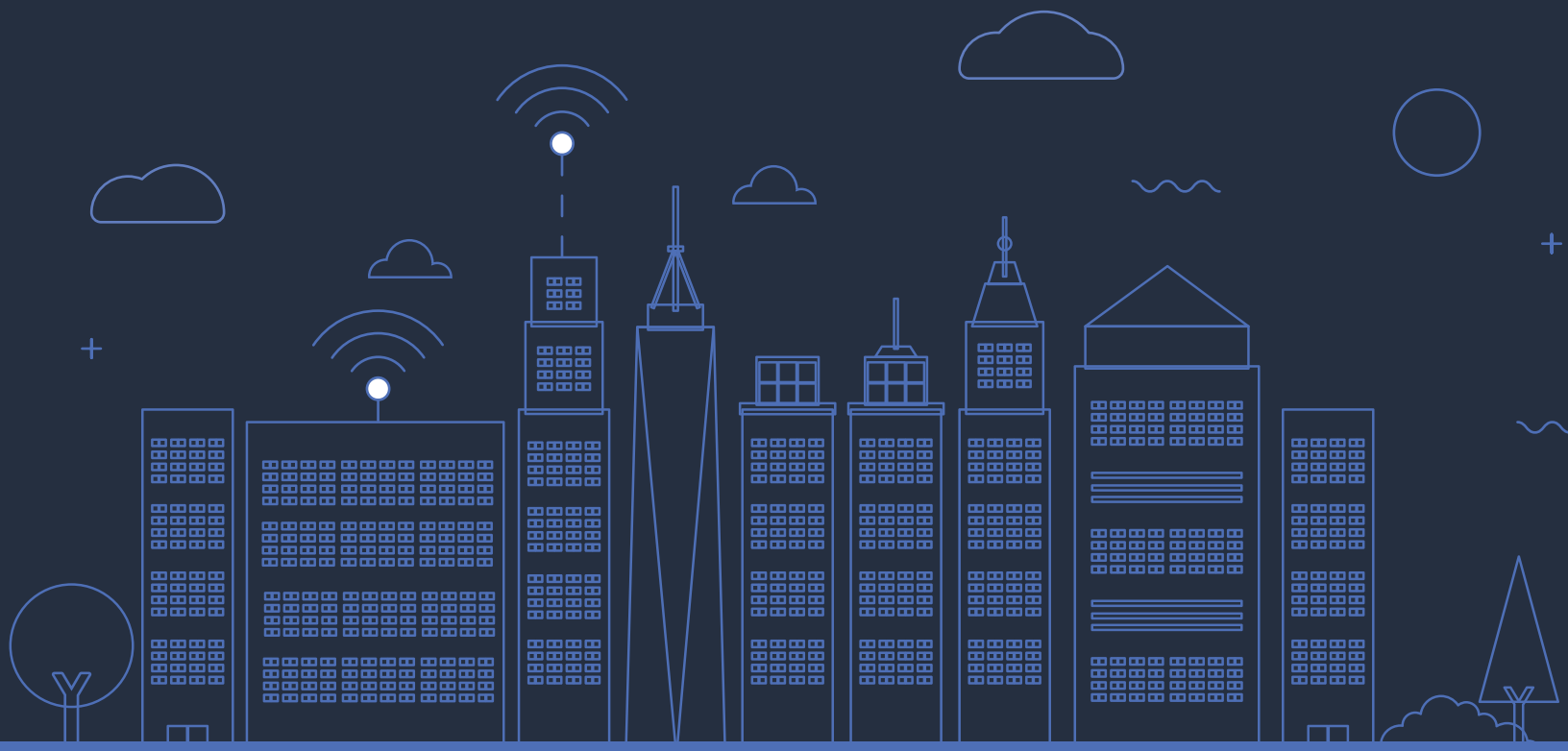
OAS Technical Team

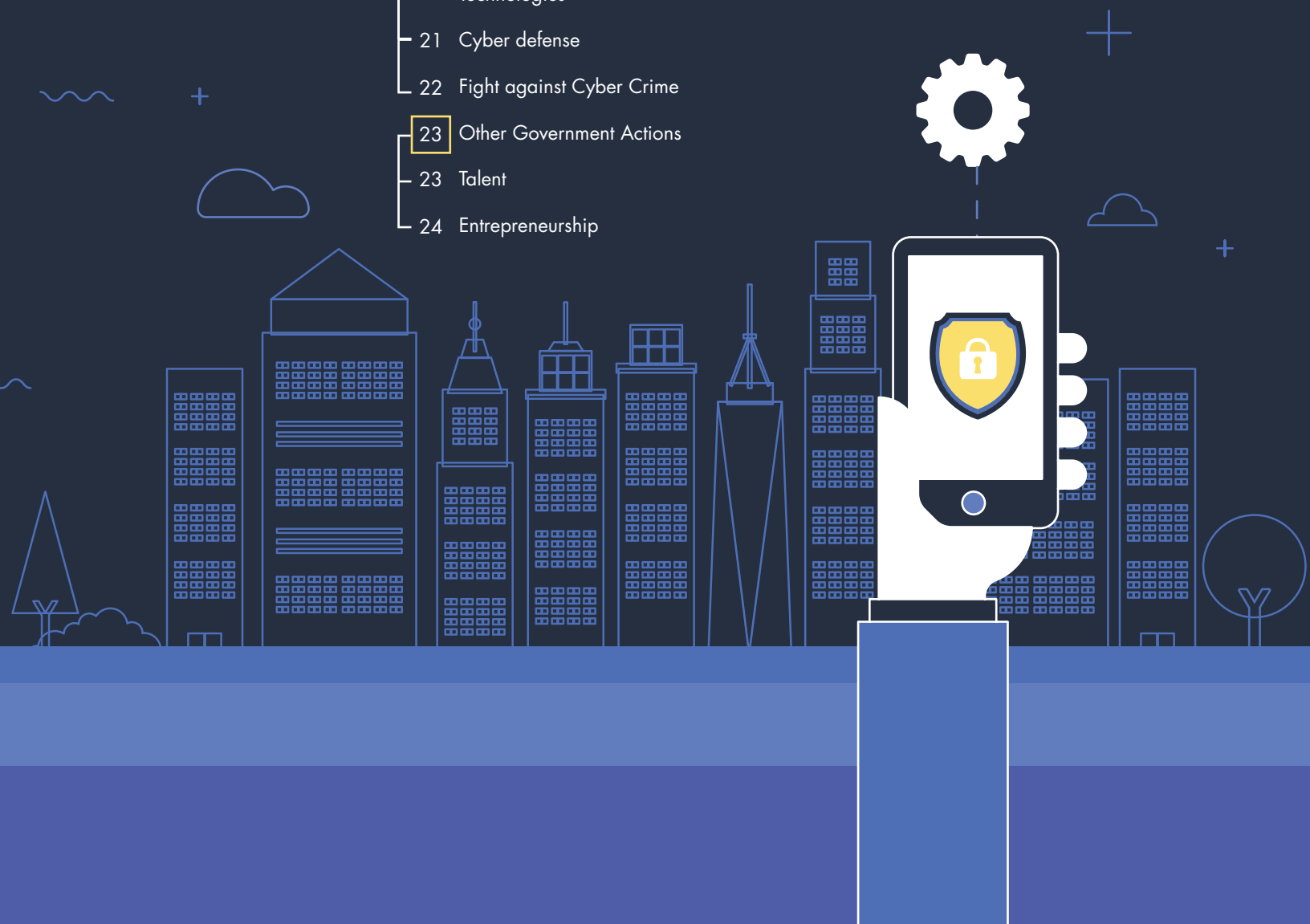
Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Nathalia Foditsch
Gonzalo Garcia-Belenguer

AWS Technical Team

Min Hyun
Michael South
Maria Saab

CONTENT





1

PURPOSE

Information and Communications technologies have revolutionized our way of life and have driven economic and industrial development to the point where we have become highly dependent on cyberspace. Our way of communicating, interacting, pursuing education and even how we purchase items has been transformed with the growing penetration of digitalization which has changed our habits and behaviors. These digital transformation processes have also impacted the public and private sector, to such an extent that any productive process or public service for citizens cannot be conceived without an intensive use of technologies.

While this scenario creates great opportunities for the economy, industry and society, it is not without new risks and threats. Cyberspace has become a great interest area for criminals and terrorists who can take advantage of the anonymity provided by the Internet and the lack of homogeneity in national and international laws, to act with impunity.

In this environment of enormous opportunities, governments must act by establishing the legal, technical and organizational conditions for their citizens, companies and public institutions to take full advantage of the possibilities of this digital reality, with the confidence to be reasonably safe.
This document aims to help identify the fundamental elements on which to support the construction of a secure digital environment that will serve the social and economic development of nations.

2 INTRODUCTION

A More Digital and Hyperconnected World

Digital transformation has meant the integration of digital technology into society including the operational aspects of many organizations. This has facilitated changes in our way of work and interactions; it has led to an improvement in industrial production processes; and has impacted economic development in a very positive way. We are becoming more digital and hyper-connected and the presence of technology in our personal and professional lives has grown exponentially.

These circumstances are enabled by the following realities:

- Massive interconnection, in what is now known as the Internet of Things (IoT), which will cause an increase from 6.5 billion interconnected elements to the Internet to more than 21 billion, and which will facilitate the monitoring and remote control of multiple smart devices.

- Internet-enabled physical systems, which is the result of providing physical components/objects with computing and communication capabilities which in turn coverts them to intelligent objects that can cooperate with each other, forming distributed and autonomous ecosystems. This trend, together with the IoT, are the basis for the development of SmartCities, and in general the SmartX, that is, the implementation of these concepts to almost any area, process or organization (cars, drones, homes, hospitals ...)

- Maximization in data storage and its analysis and exploitation. The massive amount of information created by the IoT allows the generation of predictive analysis and facilitates more efficient and productive work.

- Cryptocurrencies and blockchain, although deemed a very volatile value, have already revolutionized the way of doing business on the Internet. With the growth of implementation, in 2020 they will account for 25% of all financial operations.

E-commerce will continue to increase its quota in virtually all markets for the sake of customer convenience and for speed and reliability of deliveries.

Other trends will contribute to this unstoppable growth of "all things digital," such as artificial intelligence and machine learning and virtual and augmented reality (AR), among others.

Threats are More Complex and Evolving

Criminals are able to develop increasingly sophisticated attacks, which has been catalyzed by the increase in available attack surfaces, as more and more processes become digital. Industrial control systems (ICS) that enable the operation of essential services such as energy, water or transport, or that support industrial manufacturing process, have begun to be the target of attackers who, motivated by political, patriotic or ideological beliefs, seek the disruption and sabotage of these services.

Threats are evolving and becoming increasingly complex. Cybersecurity architectures of ten years ago served their purpose when threats and attacks were less frequent, but now these systems are becoming obsolete and need to adapt to the new threat environments. Cybersecurity requires constant innovation and investment in firewalls, proxies, WAFs and other technologies, whether on site or in the cloud, in addition to user training and security processes. The adoption of cloud computing creates additional defense alternatives given it allows greater granularity in each layer of the infrastructure, reducing the available attack surface.

The Three Pillars of Security

It is important, especially for governments, to understand that the challenges in cybersecurity will not be solved by technology alone. A complete cybersecurity strategy must cover, policies, programs, budget and implementation, i.e. the three pillars of cybersecurity: people, processes and technology.

Attackers are Numerous and Very Heterogeneous

Each day more than 230,000 different malware samples are produced and the trend is for this number to grow. Daily, more than 4,000 ransomware attacks are reported. This continuous growth in the number of attacks is motivated by the potential economic benefit the cybercriminal hopes to obtain. It is estimated that the losses associated with computer-related crimes will reach the figure of 2.1 trillion dollars in 2019.

However, unlawful enrichment is not the only motivation. Sometimes, the target of a cyber-attack can be confidential information such as the theft of military, economic or political information. In this case, attackers could be sponsored by a State or even by a company with conflicting interests with the target.

Government Networks and their Vulnerabilities

The networks and systems of governments and public administrations are a natural target for cybercriminals. Systems possess a wealth of personal information, which includes financial and banking information. In addition to personal data, public institutions handle and store confidential information that may be of high interest, for example information related to third countries, strategic interest, etc.

These technological environments could be the object of cyber terrorist attacks to block critical services and operations provided by the government or administration or be the subject of propaganda attacks or driven by social unrest.

This characteristic that attracts cyberattacks, is compounded by the fact that many network systems still operate- "legacy" systems, with discontinued or very limited support, and which coexist with more modern and advanced technologies. This situation have the potential to be high risk especially when users are poorly trained and possess little awareness of cybersecurity, and the technical personnel of systems operation and maintenance is scarce.

It is essential that organizations in the public and private sectors implement IT solutions that can respond proactively and preventively to real and perceived cyber threats. These organizations can make the most of available cybersecurity solutions that identify threats, notify service providers and implement measures that mitigate in real time.

National technological modernization plans should also be an opportunity for governments to improve the level of IT infrastructure protection. As installed infrastructure approaches obsolescence, governments can take advantage of the advanced security capabilities of newer technologies (such as the cloud) to seek out more efficient models.

Generally, the budget allotted to cybersecurity technologies and services for the protection of these environments in the public sector is usually significantly lower than those of other sectors.

3

THE ROLE OF GOVERNMENTS IN THE PROTECTION OF CYBERSPACE

The heavy dependence on cyberspace, and the growth and complexity of threats, makes cybersecurity a fundamental element for the social and economic stability of any nation and should be a matter of national priority. In this context, governments must assume a leadership role in promoting a secure cyberspace that creates trust in citizens and businesses, and facilitates the social, economic and industrial growth of the nation.

This leading role of the State translates into the following lines of action:

Formulation and Implementation of Public Policies

Governments must participate actively in forums and international organizations and in supranational structures with the aim of harmonizing and coordinating a common position for the protection of cyberspace. This effort must materialize in the signing of international agreements and in the revision and adaptation of national legislation. As a first step, government action should be translated into a national cybersecurity strategy that establishes the principles, objectives and lines of action from where a cybersecurity model for the country can be developed.

Development of a Collaborative Response

The protection and response to cyber threats involves not only the government, the administration and public institutions but society as a whole. Critical infrastructures, on which essential services depend, are largely managed by private companies that play an essential role in national cybersecurity. Companies providing cybersecurity products and services are also important because they have public and private organizations as clients, which utilizes their solutions to protect key processes and information.

Understanding that technology implementation and its use in the public sector, can be slow at times, governments should nevertheless continue to access innovative and technological solutions with sophisticated means to improve cybersecurity. As threats become more complex and malicious actors become more numerous, technology must adapt to respond effectively. The market for cybersecurity products and solutions is also evolving to offer the solutions needed to address the threats and demand.

People usually act in two-capacities, both as users of the services of information technology and as employees. Therefore, they are also essential, since their behavior with technologies can facilitate or prevent the success of a cyber incident. Additionally, universities and research centers educate future professionals and define models or solutions to current or future cybersecurity problems, which also makes them an important factor to consider.

In this context, where so many different actors contribute in a relevant manner to national cyber security, the government has to play a coordinating and harmonizing role of all these efforts towards a common goal.

Creating a Culture of Cybersecurity

It is important that the relevance of cybersecurity penetrate all levels of society and that this knowledge be translated into behavioral patterns. The creation of a national culture of cybersecurity must be promoted by the government through different means and channels, and it must involve citizens, companies and public administrations, and include a range from decision-makers to employees.

One possible example of this is the National Cyber Security Awareness Month (NCSAM), which has been implemented in many States throughout the United States of America.

Promotion of a Professional and Business Ecosystem

Improving and maintaining an adequate level of cybersecurity in companies and public institutions requires a significant number of professionals with the appropriate qualifications. In turn, information technological systems need to be equipped with cybersecurity solutions to protect them against cyberattacks. Both aspects are critical to be able to develop a national cybersecurity model.

On the other hand, the global deficit of professionals and the increase in the demand for cybersecurity products and services can be an opportunity for economic development and for improving the ability of international influence for nations that are capable of exporting cybersecurity talent and technologies.

Governments must play an essential role in the promotion of an ecosystem of entrepreneurship and the development of talent in cybersecurity, by stimulating interest in cybersecurity from the early stages of education, and encouraging and supporting the creation of ideas and projects that can lead to entrepreneurial initiatives.

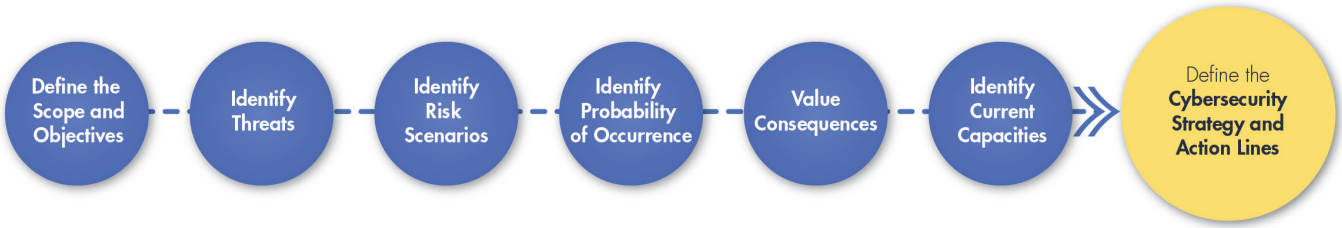
4

WHERE SHOULD STATES START?

The definition of a national cybersecurity strategy should be the first step in building a secure cyberspace. This strategy should be defined after identifying and assessing the cyber risks that could affect the country. This approach will allow:

- The protection of national interests in cyberspace against real threats that can act against them;
- Greater efficiency, which means that implemented measures would be proportional to the level of importance of the goods and assets to be protected and their actual level of risk exposure ;
- Revisiting existing cybersecurity measures and integrating them into the new model;
- The inclusion of a prioritization of the actions and the lines of action that have been defined;
- Evaluating the state of security of the types of technology most used by public and private sector organizations, and determining their level of modernization and sensitivity to cyber risks and threats;
- The inclusion, in policies, programs, funds and implementation, the three pillars of cybersecurity: people, processes and technology.

The steps to follow are:



STEPS TO DEFINE THE STRATEGY

1. . . . Define the Scope and Objectives

In this first step, the scope of the strategy must be defined, deciding the aspects to be covered: government, private sector, critical infrastructures, citizens, the academic environment, etc.

The guiding principles to govern the model should be described. These principles are based on the values and cultural aspects of society and aligned to the fundamental rights and freedoms established by the country.

2. . . . Identify Threats

In developing this phase, governments must identify and classify the different types of potential attackers and their degree of motivation. It will be necessary to seek contributions from a variety of sources, including government and law enforcement agencies, the private sector and academia. The prioritization of threats differs according to country, given that they are conditioned by the geopolitical situation, the level of economic and industrial development, and their own culture and social reality.

In general terms, threats can be classified into:

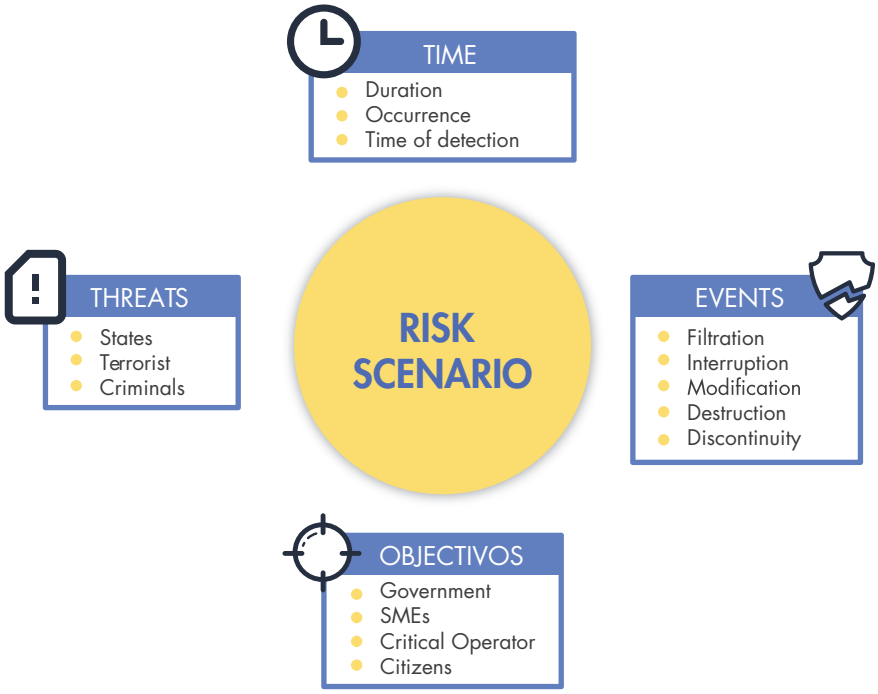
- **Cybercrime:** This includes traditional crimes that are carried out using information systems as a means or tool: fraud, economic theft, information theft, extortion, harassment, sexual abuse of minors, sabotage, etc., along with other specific offenses such as unauthorized remote access, etc.
- **Cyber terrorism:** This threat includes the actions that terrorist groups can perform through networks and systems to block critical infrastructures, to attract supporters or spread propaganda.
- **Actions from third countries:** These can range from attacks for confidential information theft to asymmetric warfare actions to block or destruct essential services.

3. . . . Define Risk Scenarios

Risk must be understood as an estimate of the likelihood that a cyber threat, whether internal or external to the country, can act against citizens, companies and public institutions, which may affect essential processes, services and technologies. When analyzing risk, threats must be considered, as well as their capacity to create damage (impacts) to the elements and interests to be protected (assets), taking advantage of certain weaknesses (vulnerabilities) in the environment or in the technologies that support it, which determines the probability of occurrence. Consequently, the risk is determined as a function that depends on these variables, succinctly expressed as follows:

Risk: f (Asset, Vulnerability, Impact)

The risk scenarios allow events that can affect the security of the cyberspace to be analyzed and national interests, providing a methodology for its assessment and management.



Nations need to define a set of risk scenarios, identifying the events that can impact their interests, identifying the potential threats that could act on them and the associated temporary factors, such as the time needed to detect them or the possible duration. These elements, objectives, threats, time and events must be combined and analyzed to identify their realism and relevance. The number of scenarios considered should be limited to a manageable number, preferably between 10 and 20.

Defining and designing relevant scenarios requires experience, a detailed knowledge of the environment and of the national reality and, more importantly, involving different angles and sensitivities: public sector, private companies, universities and research centers, etc.

4. . . . Identify Probability of Occurrence (Vulnerability)

The objective in this phase is to determine the probability of the identified scenario occurring. There are two factors that can assist in calculating the possibility of occurrence:

- **Threat Analysis:** The threat can be characterized by studying various factors such as motivation, the sophistication of the technical means that would need to be used, the level of knowledge required and the number of potential attackers.

- **Vulnerability Analysis:** This considers whether the ways to carry out the attack are sufficiently known and if they are easy to detect and correct. At this point it is necessary to highlight how the obsolescence of the country's systems and technologies can aid in the threats materializing successfully. It is important, at this stage, to perform an analysis to determine the level of digital modernization.

Taking these two factors into consideration, by examining the threats and vulnerabilities, it will be possible to extrapolate an assessment of the probability of occurrence of the scenario that is being considered.

5. . . . Value the consequences (Impacts)

The objective of this is to define the consequences if the risk scenario occurs. This assessment can be based on two factors:

- **Technical:** This consists of an assessment of the consequences from a security perspective, strictly speaking, taking into account the importance of the affected services in relation to their confidentiality, integrity or availability.
- **Non-technical:** Considerations will take into account the consequences of the occurrence of the threat to the country in terms of the impact on international commitments or with third countries, the country's credibility and image, the breach of legal obligations and the increase in the indicators that determine a "risk country".

The combination of the two factors, technical and non-technical, allows us to extrapolate a valuation of the consequences of the occurrence of the scenario being considered which, taking into account the environment and scope, can be classified in tiers:

- Tier 1: when the impact can be considered to have "strategic" consequences, because it affects the national or organizational level;
- Tier 2: when the impact is considered "operational" since it affects business objectives or service lines;
- Tier 3: when the event targets specific assets, which are affected directly (people, facilities, technologies, etc.)

6. . . . Assess Current Capabilities

After identifying and analyzing the scenarios, the next steps should be the identification and assessment of the existing capacities in the country, evaluating their level of maturity and determining how they can act in the risk scenarios identified. For this, existing models of maturity assessment could be used, adapting them to the national reality, such as the Cyber Security Maturity Model for Nations developed by the University of Oxford's Global Cyber Security Capacity Centre (GCSCC), and which has been applied by the Organization of American States (OAS). This model has already been used by the OAS, with the support of the Inter-American Development Bank (IDB), to develop the study "Cybersecurity: Are We Ready in Latin America and the Caribbean?".

The model developed by GCSCC involves the following dimensions:

1. The development of a cybersecurity policy and strategy;
2. The promotion of a culture of responsible cybersecurity behaviors among society;
3. The development of knowledge in cybersecurity;
4. The creation of effective legal and regulatory frameworks;
5. The control of risks through standards, organizations and technologies.

In order to define the maturity of each of these dimensions, the following levels have been established:

- **Start-up:** at this stage, either there is no cybersecurity maturity or it is very embryonic;
- **Formative: some elements of the dimension have begun to grow and be formulated, but they are ad-hoc;**
- **Established:** some elements are in place and are working. However, well-thought out allocation of resources is not considered;
- **Strategic:** decisions have been made about what parts of the dimension are important and less important; these choices are made contingent on the particular circumstances of the nation; and
- **Dynamic:** there are clear mechanisms to modify the strategy depending on prevailing circumstances.

The review of the actual level of maturity of national cybersecurity capacities, allows us to understand the real level of risk of the identified scenarios and to determine the requirements to be included in the national cybersecurity strategy and its development.

7. . . . Define the National Cybersecurity Strategy and Lines of Action

The National Cybersecurity Strategy is the document that describes the objectives that must be achieved to manage cybersecurity risks comprehensively from a national perspective. It should include all relevant considerations for the identification and analysis of risks, and it should serve as a lever to boost necessary national capacities in cybersecurity and cyber defense.

National strategies should be "living" documents, reviewed and updated periodically and designed in collaboration with all public and private stakeholders that may be interested. It is essential that the national strategies reflect the social values, traditions and legal principles in the country and should cover the dual objective of being both the basis of the national cybersecurity model, as well as a catalyst to facilitate the transformation of the country's digitalization.

Finally, the strategy must include lines of action to allow the government to implement the activities for which it has the responsibility to execute and to meet the defined objectives with the goal of managing the risk scenarios identified.

5

HOW TO CONTINUE? FROM STRATEGY TO ACTION

After the definition of the strategic objectives in the national cybersecurity strategy, and the development of the lines of action, governments should develop legal and regulatory instruments, assign roles and responsibilities and build the necessary technical and organizational capacities to move from strategy to action.

Actions for the Citizen and the Private Sector

Awareness-raising activities should be promoted to ensure that citizens and businesses are aware of the vulnerabilities and possible cyber threats that exists and be given the know- how to incorporate an adequate pattern of behavior into the use of technologies and the Internet. "Cyber hygiene", (that is, education towards correct behavioral models that prevent the adverse effects in the use of technologies) could be promoted through the following:

- Communication campaigns in the media aimed at citizens and small and medium enterprises (SMEs), to promote the safe use of the Internet, encouraging the adoption of tools and disseminating "cyber-hygienic" practices.
- Awareness and education programs in collaboration with public and private sector actors, seeking coordination and rationalization of efforts.
- Develop educational modules aimed at all education levels.
- Create or encourage the development of events at national, regional or municipal levels, and include workshops to promote good practices in all users and in specific groups such as parents, educators and minors.
- Develop and share attractive multimedia content and educational tools based on "gamification".

Special attention should be given to the prevention of cyberspace risks where minors are victims. Governments should design an educational and content program specifically aimed at preventing and detecting cases such as cyber bullying, sexting and grooming, for example, and also establish a specific channel for reporting, controlling and monitoring these cases.

With respect to the private sector, the government could carry out the following specific actions:

- Facilitate the use of solutions for the exchange of information on threats, vulnerabilities and incidents between companies of the same or similar sector, so as to create a collective intelligence that will allow preventive and timely responses to incidents.
- Develop good practice codes and support the development of certification standards.
- Promote cyber exercises to test coordination mechanisms between different companies and with public agencies and improve the effectiveness in incident response.
- Develop comparative studies between entities of the same sector and geographical area, with the aim of defining baselines and benchmarks.

The government should promote the creation of a national capacity to respond to cyber-incidents (e.g. a Computer Incident Response Team (CIRT) to provide specific services for citizens and the private sector. This capacity should be complementary and never compete with the services provided by service providers through private CIRTs or Security Operations Centers (SOCs). The objective of this public CIRT is to develop valuable services for the management and implementation of national crisis situations or for services that respond to the following characteristics:

- Incidents that are of extreme importance for national security and defense.
- Value services for national cybersecurity, which are not being covered by the private sector due to low demand or because they are not profitable.

It is essential, therefore, for government to have a detailed vision of the different market players and the services they are providing, with the aim of seeking synergies and avoiding overlaps.

Actions for Critical Infrastructure Operators

The protection of critical infrastructures must be a fundamental part of the national cybersecurity strategy since it aims to optimize the resilience of the infrastructures on which essential services for the nation depend. The cybersecurity of public or private organizations that operate these strategic sectors is of particular importance given that a successful cyberattack on them can have a very serious impact on security and the functioning of the country. This impact could affect the lives of citizens, the stability, strength and credibility of the economy or international reputation.

The actions that governments could promote for the protection of these types of organizations are:

- To define and identify critical sectors. The government should determine the critical sectors that are of national dependence, the unavailability of which could have serious consequences. Countries have developed different approaches based on their geopolitical, economic and industrial conditions, but there are certain sectors that appear in all national models: Public Administrations, Energy (Electricity, Gas, Oil, Nuclear Energy), Transport (Rail, Roads, Air and Maritime), Finance (Banking and Payment systems), Water, Telecommunications Networks and Health.

- To develop a method to identify and assess critical infrastructures, so that these criteria are uniform and repeatable over time.
- For each of the strategic sectors, the government could define: the catalog of threats, the specific criteria when identifying whether the services provided by a certain organization should be considered critical and the catalog of operators and critical infrastructures.
- The minimum-security requirements that critical operators must implement, the risk assessment model and cybersecurity governance and management.
- To facilitate mechanisms for the exchange of information among operators on incidents and threats.
- To define, for national CIRT or CIRTs, a catalog of specific services for critical operators. This catalog should respond to the singularities of each strategic sector considered: threats, services and technologies on which they depend, consequences and impacts of non-functioning.
- To promote sectoral cyber exercises to improve the readiness degree of the operators when facing systemic cyber-attacks. These exercises, singular and specialized, should be complemented with other intersectoral exercises, focusing on preparing for crisis situations at the national level.
- To promote events and other forums that facilitate knowledge and exchange of experiences among those responsible for cybersecurity, as well as encourage the creation of sectoral working groups to promote and develop specific security models for each sector.
- To know the specific product and service needs of the operators of strategic sectors is very useful in order to determine whether the current supply offered by the market is adequate. This knowledge can be used by the government to guide academic research and to serve as encouragement to the development of entrepreneurship initiatives.

Actions for the Government and Public Institutions

The government and public administrations must have a high level of protection against cyber threats. This rationale is based on the following considerations:

- The search for greater efficiency in the operation of public services and greater proximity to citizens has prompted many governments to adopt digital transformation processes in public administrations, which has been called eAdministration or eGovernment. These initiatives depend on the progressive change of the way people relate to the government and adapt to this new digital reality. One of the most important elements for this is "digital trust", understood as the attribute where citizens are convinced that their data is private, secure and managed transparently. Without digital confidence, eAdministration or eGovernment is not viable.
- Public institutions process and store personal data of citizens. Therefore, they need to store this information in large databases that automatically become of interest to cybercriminals.
- In addition to personal information, the government handles classified information of high strategic value for national interests that requires additional protection measures.

Protection of Public Technologies

The actions that governments could promote are:

- To establish a national cybersecurity framework for public administrations that serves as a reference for all and that enables unifying criteria among the national, regional or state governments and local councils and administrations. The national framework, (which should include policies, procedures and technical standards, baselines, methodologies and tools), should facilitate improving the protection of public services, information and the information and communication systems it supports. Each country should adopt an industry framework as its base (e.g. ISO , NIST, etc.), and then provide guidance on how that framework will be applied in each country. It would be very difficult for companies and service providers to follow a framework and standards unique to each country, which would limit who these countries can use. Common cybersecurity frameworks, risk management, security controls, etc. will benefit the commercial sector and the government.

- To develop multinational agreements or trade agreements that facilitate the exchange of information and coordination/cooperation of countries that fight against cyber threats.

- To develop training and awareness plans aimed at public officials with the purpose of showing them the specific threats that can affect the cybersecurity of public services, and instill cyber hygienic behavior patterns.

- To develop and implement horizontal cybersecurity capabilities that bring together, and maximizes the prevention, detection and response to cyber incidents in the central, regional and local administrations. These horizontal capabilities have the advantage of unifying and standardizing cybersecurity service in all public institutions; they provide efficiency by relying on economies of scale; and allow a holistic vision that provides intelligence and valuable information.

- To develop a cybersecurity scheme to facilitate the formal evaluation and certification for the products and systems that will be part of the technological infrastructures that support the administration's essential services. To take advantage of existing international and industry standards such as SOC, ISO, PCI, NIST, etc. instead of creating its own unique standards that can be very difficult or impossible to implement.

- In addition to these activities, to defend the networks and systems on which public services are supported, governments should act to develop their capacities for cyber defense and for the fight against cybercrime.

Cyber defense

Cyberspace provides a new platform of operations and this means that, in an armed conflict, military actions can affect critical systems, information and services, so it is necessary that the Armed Forces have specialized units for the defense of national interests in cyberspace.

The actions that governments could promote to develop their cyber defense capabilities are:

- To develop specific specialization and training plans in the subject, to allow the armies to have the necessary members.
- To define a collaboration model with specialized companies and experts in cybersecurity to reinforce the capabilities of the armed forces in the cases defined.
- To promote periodic cyber exercises that facilitate continuous training on real scenarios.
- To develop knowledge and experience about threats and vulnerabilities related to cyber defense and also methods of attack, through national and international information exchange.
- To establish a cooperation with the main academic and R&D institutions for the development of specific needs in the field of cyber defense.

Fight against Cyber Crime

The fight against cyber terrorism and cybercrime must include two perspectivesw: cyberspace as a tool that enables the development of these criminal activities; and cyberspace as the end goal of the action. This requires the collaboration of different actors and it must be addressed comprehensively. The government could then act on two fronts:

- Legal, creating specific laws and adapting existing ones to allow for the prosecution of cybercrime.
- Developing capacities and providing specialized resources to the institutions responsible for monitoring compliance with the law: judges, prosecutors and police investigation units.

Governments could undertake, among others, the following actions:

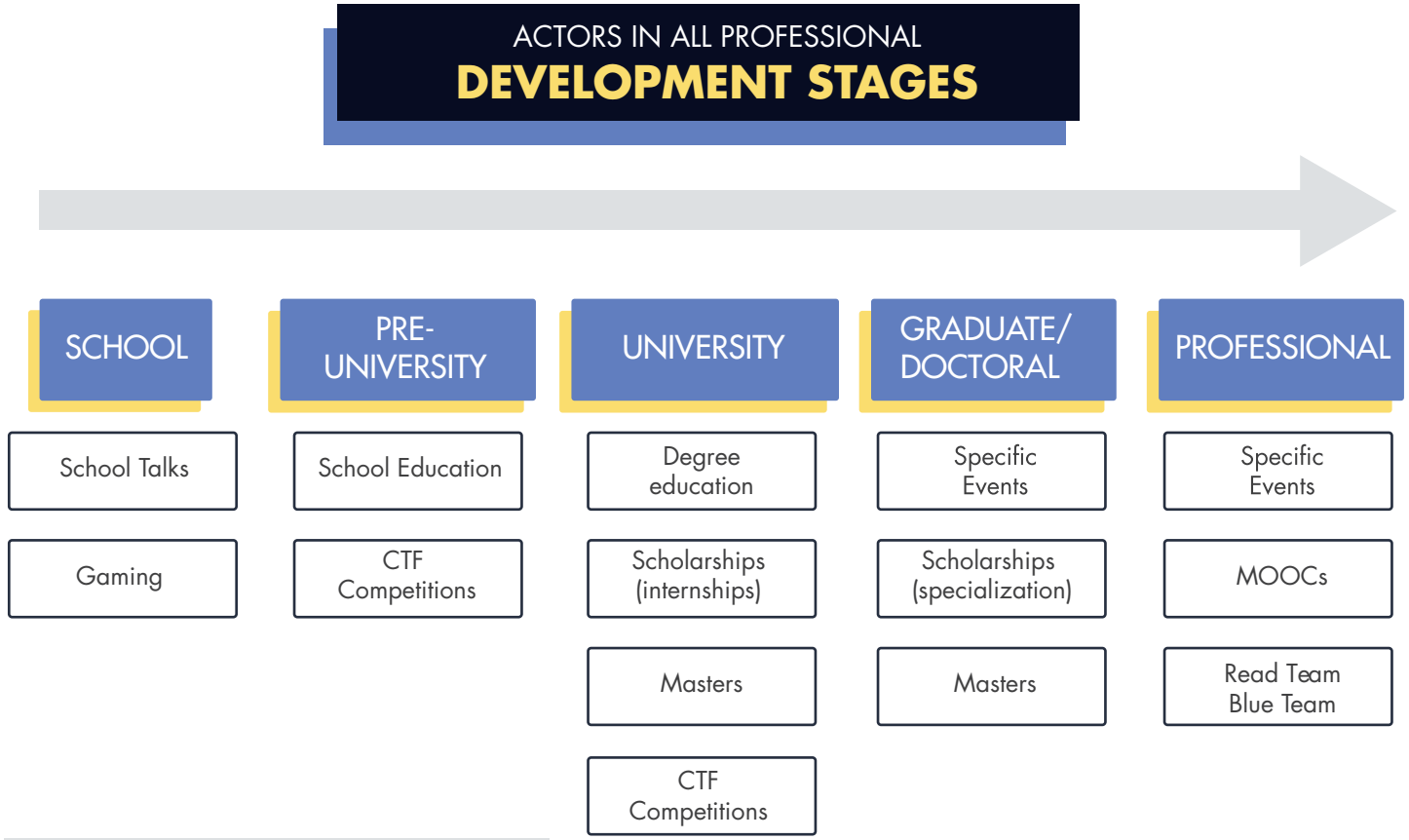
- To adapt the national legal framework to new types of crime and adapt existing types to the digital reality.
- To participate internationally in the preparation of agreements and treaties for the prosecution of cybercrime, ratifying them once approved.
- To create specialized cybercrime units (police and judicial) and develop training plans and continuous training.
- To improve the capabilities of the competent agencies and ensure coordination through the exchange of information and intelligence.
- To strengthen international police cooperation and their presence in forums and international organizations focusing on the fight against cybercrime.
- To develop knowledge and experience about threats and vulnerabilities related to cybercrime.

- To establish cooperation with the main academic and R&D institutions on new police investigative techniques.
- To establish cooperation between public and private sector stakeholders to quickly identify and respond to issues related to cybercrime.
- To create a specialized channel for citizens and companies to report possible cybercrimes.
- To develop and implement specific actions to detect and prosecute cybercrimes that affect minors.

Other Government Actions

Talent

The construction of a national cybersecurity model requires that the government, public administrations and the private sector have an adequate number of professionals with knowledge and specialization in cybersecurity. The demand for professionals grows progressively due to the fact that digital transformation processes have resulted in an increase in cybersecurity units as the dependence on information technologies and cyberspace increases. In addition, universities and training centers are not being able to absorb this increase in demand and do not generate a sufficient number of professionals. Also, the high specialization of the professional profiles demanded is not always being covered by the existing training programs.



THE CYCLE OF CREATING TALENT

Some of the actions that the government could take to improve this reality are:

- To determine the professional needs of the private and public sector, and the knowledge and specialization requirements.
- To define a general catalog of professional roles that includes the skills and competencies that adapt to technological innovation.
- To participate in the dialogue with universities and other educational institutions to develop new programs or adapt them to the needs of the labor market.
- To promote workshops and other activities in colleges and schools that stimulate interest and curiosity in cybersecurity.
- To organize cybersecurity events that help identify national experts.

Entrepreneurship

Periodically we are faced with new forms of attacks that use techniques and methods different from the ones known. This fact, together with the continuous evolution of technologies and their application in industry and society creating new cases of use, means that governments face an increasingly threatening environment, which is sophisticated and evolving. The tools and cybersecurity products of the present, cease to be useful in these new environments that can only be managed with new and different approaches. Research, development and innovation are necessary for the development of effective solutions that respond to new types of attacks.

In order to achieve this objective, governments should exercise leadership and coordination among all interested agents:

- The sophisticated demand, understood by those sectors (government, banking, energy, etc.) that either because of the degree of digital penetration in their businesses, or because of the type of threats that affect them, require novel solutions.
- Universities and innovation centers, which are the organizations that dedicate resources to technical-scientific research.
- Entrepreneurs and startups, which have ideas and projects, that can contribute to respond to these needs.

The actions that governments could develop to create an ecosystem for entrepreneurship in cybersecurity are:

- To determine, through forums and working groups, considering the sophisticated demand, the present and future needs of cybersecurity products and services, transferring this need to a national research agenda that marks the road map of research and entrepreneurship.
- To create a research plan to avoid overlaps between the research activities undertaken by different institutions.

- To establish specific funds that support cybersecurity research programs.
- To enable mechanisms to guarantee transfer to the industry.
- To encourage entrepreneurship culture among young people through an action plan that includes activities that facilitate education and guidance.
- To create ideas in line with the research agenda, competitions where young entrepreneurs present projects or prototypes that can solve problems.
- To create public funds that help entrepreneurs in the early phases of the entrepreneurship cycle.
- To create events that facilitate contact between entrepreneurs and private investment.
- To promote the implementation of startup incubation and acceleration programs (emerging companies with growth potential).

6 CONCLUSIONS

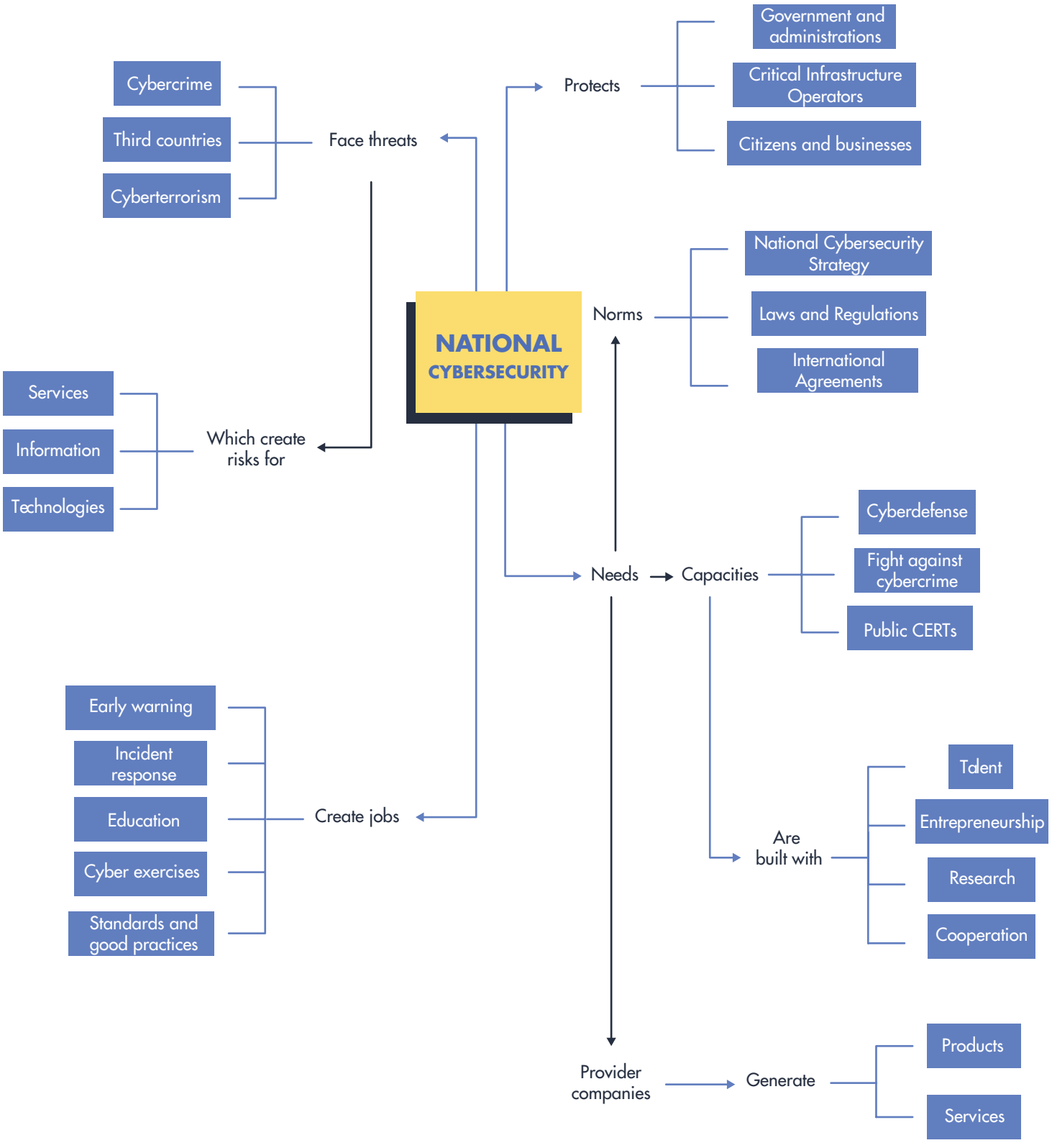
Cyberspace and technologies are a growth engine for the economy, a driver of industrial development and they have revolutionized our way of life. The way we relate to other people, how we buy or how we do business has been changed with the digital transformation processes of the present and will continue to change with the transformation processes that the future will bring us. This scenario of enormous opportunities is not risk- and threat-free, as has happened with other great advances in the history of mankind. Governments have the responsibility to define the conditions so that cyberspace and technologies can be used with reasonable levels of security, in the same way that they have been acting to guarantee public and citizen security in the face of traditional crime or legal security in the relationships between parties.

Government efforts must be based on collaboration and cooperation. In the international sphere, they could participate in international forums, adopt international agreements and establish lines of bilateral collaboration with other countries. Within its borders, governments could establish effective coordination with all public and private agents, in order to understand and address their risks and threats.

Government must understand the fundamental role played by citizens and, in particular young people, in the security of cyberspace, and it is necessary to promote a generation with a global culture of cybersecurity that leads to patterns of "cyber hygiene" behavior.

Finally, the government must aid in the creation of talent and new companies, understanding that these activities are not only an essential strategic element for the construction of the national cybersecurity model, but also an enormous opportunity for growth and development.

For all this, the first step that a government should address is the definition of a national cybersecurity strategy.



NATIONAL CYBERSECURITY MENTAL MAP

7

REFERENCES

Publications

- Amazon Web Services Risk and Compliance 2017
- National Cyber Security Strategy Good Practice Guide-ENISA
- Cybersecurity Capacity Maturity Model for Nations (CMM) Global Cyber Security Capacity Centre. University of Oxford
- Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean. -OAS 2016
- Microsoft National Strategies EN 2013
- OCDE cybersecurity policy making
- National Initiative for Education-NIST 800 181
- United States- The National Security Strategy 2017
- Estonian National Cyber Security Strategy 2014 to 2017
- UK National Cyber Security Strategy 2016 to 2021
- Estrategia de Ciberseguridad Nacional de España 2013
- 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk. - Center for Cyber Safety and Education (ISC2)
- Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017.- Sans Institute
- General Data Protection Regulation (GDPR) (EU) 2016/679 of the European Parliament and of the Council
- Directiva de Seguridad en Redes e Información (UE) 2016/1148 Del Parlamento Europeo y del Consejo
- WEF Global Risks Report 2018

Websites

- www.oas.org
- www.incibe.es/cybercamp
- www.dhs.gov/national-cyber-security-awareness-month
- www.staysafeonline.org/ncsam
- www.cyberspark.org.il
- www.cyberseek.org
- www.europeancybersecuritychallenge.eu
- www.renic.es
- www.stopthinkconnect.org
- www.oxfordmartin.ox.ac.uk/cybersecurity
- www.aws.amazon.com/whitepapers/overview-of-risk-and-compliance
- www.thebestvpn.com/cyber-security-statistics-2018
- www.eugdpr.org

OAS More rights for more people

aws

A CALL TO ACTION
TO PROTECT
CITIZENS THE PRIVATE SECTOR AND GOVERNMENTS

White paper series

Issue 1

2018