Committed To Defence And Security Worldwide

DEFENCE & SECURITY ALERT

AUGUST 2021 | VOLUME 12 | ISSUE 11 | ₹150

The First and Only ISO 9001:2015 Certified Defence and Security Magazine in India

The Only Magazine Available On The Intranet Of Indian Air Force

www.dsalert.org

info@dsalert.org

NEED OF NATIONAL COUNTER-TERRORISM CENTRE (NCTC)

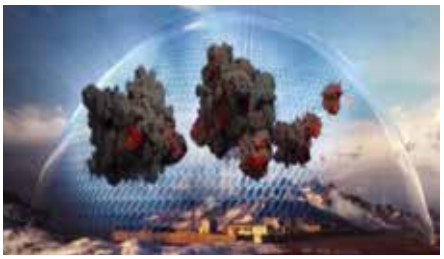
CYBER-WAR
THE INVISIBLE THREAT

DSA™

THE FIRST CHOICE IN THE DOMAINS OF
DEFENCE, SECURITY AND WORLD AFFAIRS
WORLDWIDE

11 YEARS OF EXCELLENCE

ISSN 0974-20kX



NATIONAL CYBERSECURITY STRATEGY : A NECESSITY

Those nations unable to adequately implement and manage cybersecurity measures to counter cyberattacks will undoubtedly be doomed to failure.

The 21st century has transformed our way of life, creating a globalized, hyper-connected society that highly depends on telecoms. The internet and new technologies are increasingly becoming more important in our daily lives, blurring boundaries between the physical and digital worlds. This massive technology innovation has also generated a whole new world of unprecedented opportunities, such as the internet of things (IoT), artificial intelligence, cloud computing, robotics, blockchain, biotechnology, etc. All this has caused a great impact on business environments and also generated countless new professions.
The COVID-19 pandemic has also sharpened the digital transformation, accelerating the implementation of the so-called "teleworking", thus making citizens even more dependent on technologies to survive.

However, despite the undeniable opportunities that technologies can bring for the well-being and prosperity of citizens, they also bring multiple risks that can materialize into real threats, raising uncertainty and distrust among the population. One of the threats that will have the

The use of cyber world is increasing day by day, it has also become one of the most important aspects of technology after Covid-19.

greatest impact on every country in the upcoming years will be attacks targeting computer and telecommunications systems, also known as “cyberattacks”. The variety of these attacks and the actors promoting them are becoming complex and diverse. The interests behind the attacks range from simple economic motivation of small criminal organizations to cyberwarfare funded by governments against their political rivals. Some cyberattacks can also cause a major impact, such as those targeting the critical infrastructure of nations, with serious consequences for the flow of electricity or water supplies or the functioning of essential services. Cyberattacks are not only limited to actions that can jeopardize infrastructure security or information asset confidentiality, integrity and availability. They can go much further: disinformation campaigns (fake news) that can tamper public opinion and electoral processes, financing of terrorism and recruitment and massive espionage of citizens through the theft of information, among many others.

Citizens, companies and organizations, in general, should be able to navigate cyberspace securely and it is the responsibility of all nations to guarantee this right. Therefore, all necessary measures must be adopted to achieve a level of cybersecurity that minimizes the impact of cyberattacks as much as possible, allowing societies and nations to prosper. States and public authorities must ensure that the digital transformation process is carried out with utmost security and efficiency, and minimize disruption towards citizens. Every nation must provide all the necessary resources to guarantee a secure cyberspace.

For all these reasons, nations wishing to survive in the new digital world and ensure the prosperity and well-being of their citizens must have a consolidated and coordinated National Cybersecurity Strategy. For such a purpose, strategies should not only guarantee the security of critical national infrastructures and strategic information assets, but also foster a cybersecurity culture, strengthen judicial capacities and improve international coordination, among many other aspects. All this represents a complex and multidisciplinary challenge, which should include at least the following strategic lines:

1. Develop and implement the necessary capabilities to mitigate cyberattack risk exposure.

The security and resilience of critical national infrastructures and strategic assets must be ensured by providing all the resources (both technical and human) that can provide a secure cyberspace. This requires maximizing capabilities aimed at managing the entire cyberattack lifecycle, including prevention, detection, response and recovery from attacks directed against essential services and strategic assets (see public sector information as well as the networks and IT systems that support them). The security strategy should have an approach based primarily on technology risk management and appropriate management of vulnerabilities and associated countermeasures. It is highly recommended for cybersecurity operations to be centralized at national level to improve execution, coordination and response times to any incident. The development of regular cyber exercises with an eminently practical and operational approach will also ease security incident management.

It is recommended to develop and implement quantitative

Every **nation** must provide all the **necessary resources** to guarantee a **secure cyberspace**

ANTONIO DELGADO

The writer is Cybersecurity and IT Risk Consultant in Capgemini, with vast experience in multiple projects for companies in the Financial, Insurance, Logistics, Energy, and Automotive industries, among others. His main lines of work include Risk Analysis, Regulatory Compliance, Business Continuity, Disaster Recovery, Security Operations and Communication and Network Security. linkedin.com/in/amdelgadoalonso

systems that use metrics to evaluate cybersecurity maturity levels, facilitating the detection of those areas that present greater opportunities for improvement and allow for corrective actions to be applied more easily. It is recommended to promote the creation and dissemination of best practices as well as collaboration between centers of excellence and reference to build a cybersecurity culture among operating staff and management. The development of cyber-intelligence platforms will allow for the exchange of information and notifications on threats, trends, etc. The support and dynamization of the cybersecurity technologic industry will be another essential part of any self-respecting National Cybersecurity Strategy.

The development of products to strengthen the cybersecurity of nations as well as technological research should be supported as much as possible.

2. Promote a cybersecurity culture within the business network and society.

Another of the main axes on which national cybersecurity strategies should be based is the promotion of the so-called "cybersecurity culture" both in society and in the business network. Citizens must be aware of the main risks to which they are exposed when using new information technologies and must use them safely and responsibly. To this end, the necessary knowledge, skills and technological and professional abilities must be fostered so that citizens know how to face the great challenge posed by the current digital revolution and the new panorama we are living in. The culture of collective cybersecurity must be promoted by both public and private institutions through regular training initiatives according to the different levels of knowledge of citizens. Cybersecurity must always be adapted to the target audience's understanding, from the newer generations that are more familiar with digitalization to those that are not so aware of this reality (see senior citizens). SMEs, the backbone of economy, should be another key target of cybersecurity training actions. It is recommended to encourage the creation of cybersecurity forums involving the main public and

Strategies should not only **guarantee the security** of critical national **infrastructures**

private representatives in order to maximize cybersecurity training and awareness. Professional training will be another of the main pillars on which the promotion of the cybersecurity culture must be based, promoting specialized qualifications in university environments, certification schemes and the generation and exchange of knowledge.

3. Strengthening the judicial framework for cybersecurity.

These measures are aimed at strengthening cybersecurity but they can also be undermined without a legal framework that responds effectively to criminals, threats and a constantly evolving technology environment. It is therefore necessary to strengthen and improve investigation and prosecution capabilities against criminal actors involved in cyberattacks. Furthermore, legal frameworks need to adequately support criminal prosecution, attribution and regulation in investigations, providing all actors involved with the necessary legal tools to protect nations and their citizens from cybercriminals.

The frenetic pace at which both cyberattacks and the technology that supports them are changing and evolving requires a constant dialogue and exchange of information between the judicial and technological sectors to make sure that they are on the same page.

The global and transversal nature of the internet will also require international judicial and police cooperation, setting common action and collaboration frameworks.

The exchange of intelligence and experience between nations, as well as those actions that will require international collaboration efforts, will become increasingly common and necessary.

Secured Cyberspace

Nations wishing to survive in the new digital world and ensure the prosperity and well-being of their citizens and business sector must guarantee a secure cyberspace. The ever-increasing number and complexity of cyberattacks brings out the need for a National Cybersecurity Strategy to guarantee the security of critical infrastructures and strategic information assets through efficient technology risk coordination and governance.

The provision of the necessary resources (both technical and human), the promotion of a culture of cybersecurity and the strengthening of judicial capacities to combat electronic crime will be the essential pillars for the success of these strategies. All this will represent a complex and multidisciplinary challenge that will have to face a constantly changing and evolving world. Those nations unable to adequately implement and manage cybersecurity measures to counter cyberattacks will undoubtedly be doomed to failure. DSA