CALL FOR

Government Action on Cybersecurity

ICC CYBERSECURITY ISSUE BRIEF #1

EXECUTIVE SUMMARY

The global business community has made significant and continuing investments in securing technologies and developing defensive cyber tools, skills, and procedures. Despite these major contributions, industry cannot bear the growing destructive consequences of cyberattacks alone. To substantially curb the ever-rising trend of cyber threats, both in the probability of occurrence and in its organisational and social impact and incidents, urgent and concrete actions are needed by governments—on the national and international fronts.

The International Chamber of Commerce and its members call on governments worldwide to:

- uphold and implement commitments to international law and norms;
- adopt a multistakeholder approach to inform policies and to help protect critical infrastructure;
- bolster cross-border cooperation to effectively tackle cybercrime;
- curtail the proliferation of offensive cyber tools and instruments;
- invest in capacity building to understand cyber-risks and cyber-exposed assets and their vulnerabilities; and
- support the private sector's efforts to systematise a prevention first approach to cyber threats.

CONTENTS

INTRODUCTION

In 2020, the annual cost of cybercrime to the global economy was estimated at a staggering €5.5 trillion, double that of 2015. This represents the largest transfer of economic wealth in history, greater than the global drugs trade.[1] Non-monetary costs are also on the rise as the public becomes acutely aware of, and increasingly concerned about cyberattacks. In a 2021 report[2], citizens of 28 countries surveyed across the globe stated that their fear of cyberattacks is on par with their fear of contracting COVID-19. Similar feelings were expressed in a separate report[3], in which 84% of people interviewed consider the threat of cyberattacks to be on par with the threat of nuclear weapons. These fears can result in painful psychological costs to individuals and their communities, and directly and indirectly create challenges for businesses and governments, as discussed below.

Cyberattacks take many forms. We continue to see wide-scale exploitation of personal technology and information focusing on data theft and alteration, phishing, and ransomware. However, malicious actors are also now targeting innovations that power the 4th Industrial Revolution, and with potentially destructive consequences. Cyberattacks on critical infrastructure—rated the fifth greatest risk in the 2020 World Economic Forum Global Risk Report—have become the new normal across sectors as essential as energy, healthcare, utilities, and transportation. Such attacks have been seen to affect entire cities and communities.[4]

Alarmingly, cybercriminals are not the only nefarious actors citizens and the business community must defend against, there is also a growing number of states investing and working in destabilising activities in cyberspace. States increasingly view and consider technology and cyberspace as an area of geopolitical competition, and the number of states with the ability and willingness to conduct sophisticated online/offline cyberattacks has grown steadily. States or state actors now combine traditional cyberattacks (such as malware, phishing, man-in-the-middle (MitM), or distributed denial of service (DDoS) attacks) with disinformation campaigns into complex hybrid threats that sow mistrust and often weaken social cohesion, while also negatively impacting economies. These activities have undermined international security and stability, and increasingly jeopardized communities' abilities to seize and leverage the tremendous benefits that cyberspace can generate for economic, social, and political development.

Several serious cyberattacks have recently demonstrated to the public their very tangible and consequential impacts. Attacks on hospitals immobilised procedures in the middle of the pandemic, and a cybercriminal gang used ransomware to disable the Colonial Pipeline for several days, creating a petrol shortage that almost ground the east of the United States to a halt. In early 2020, a key US information technology firm, SolarWinds, was the subject of a large and sophisticated cyberattack that went undetected for months after spreading to their clients (including Fortune 500 companies and numerous US federal agencies), impacting up to 18 000 customers. In the first months of 2021, four zero-day exploits were discovered in on-premises Microsoft Exchange Servers. Attackers gained administrator privileges on servers, giving them access to users' email addresses and passwords on affected servers, as well as access to connected devices on the same network. It is estimated that 250 000 servers fell victim to the attacks, including servers belonging to around 30 000 organisations in the United States, 7 000 servers in the United Kingdom, as well as the European Banking

[1] European Commission, JRC Publications Repository - Cybersecurity, our digital anchor (europa.eu), 2021

[2] Edelman, Trust Barometer, 2021

[3] Digital Peace Now, Cyber Awareness Report, 2020

[4] World Economic Forum, Global Risk Report, 2020

Authority, the Norwegian Parliament, and Chile's Commission for the Financial Market. These highly publicised events are just a few examples of the barrage of attacks the private and public sectors face on a recurring basis due to the rapid and pervasive progression of malicious activities.

Bold and decisive action to curtail these activities is no longer an option, it is a necessity. The private sector invests heavily in developing and deploying secure technologies. Current trends related to the spending on cybersecurity will surpass $150 billion in 2021, an increase of 12.4% over the previous year.[5] In addition, businesses spend significant time supporting and collaborating on initiatives to promote norms for responsible uses of technology and information. Examples of launched initiatives include the Global Forum on Cyber Expertise, the Cybersecurity Tech Accord, the Paris Call for Trust and Security in Cyberspace and the Internet Society MANRS initiative. However, despite their considerable efforts, the business community and governments continues to be exposed to unacceptable and growing criminal and state sponsored malicious cyber activities.

Governments must take action to control and help reverse the tide of deteriorating cybersecurity and cybersafety conditions. This Issue Brief addresses (i) the expanding cybersecurity risk landscape with which businesses must contend, (ii) the wider economic and social impact of cybersecurity threats on the business community and communities more widely, and (iii) the urgent steps that governments must take to curb cyber threats and shield their citizens and economies from the destructive consequences of cyberattacks.

PART 1: An expanding cybersecurity risk landscape for businesses

Protecting cyberspace is becoming increasingly harder to achieve as more and more of our lives become connected—through smart homes, smart factories and now smart cities. The high level of connectivity and tightly woven set of interdependencies between critical infrastructures and non-safety certified embedded software is creating more threats and vulnerabilities than ever before. With a projected 67 billion IoT endpoints[6] expected to exist by 2025, the attack surface to our critical IoT infrastructure has never been so great, nor grown at such an exponential rate.

Malicious cyber activity impacting businesses continues to rise in scale, frequency, and complexity. More than 350 000 new malware variants are released every day, offering hostile cyber actors nearly unlimited options of offensive cyber capabilities (OCC). The growth in OCC has been spearheaded by the proliferation of both tools and services offered throughout the dark web. Consequently, an increase in ransomware attacks has been further exacerbated by a new model known as Ransomware-as-a-Service[7] (RaaS), where sophisticated cyber criminals provide easy off-the-shelf access to ransomware tools to any individual or group at low cost. This has significantly lowered the barriers to entry into this lucrative criminal market[8], fuelling growth in attacks' complexity and frequency and increasing the potential destructiveness of attacks as inexperienced attackers are given access to extremely sophisticated tools.

[5] https://venturebeat.com/2021/07/18/what-to-expect-for-cybersecurity-investment-as-we-emerge-from-the-pandemic/

[6] Professional Security, IoT Scale, 2021

[7] Blackberry, Threat Report, 2021

[8] Washington Post, Global Losses Cybercrime Skyrocket, 2021

Botnet attacks are constantly evolving and becoming more sophisticated.[9] In the early 2000s, criminals mainly used botnets for rudimentary DDoS attacks, but today's cyberattackers often conduct malicious activities on a much larger scale. For example, in March 2021 "the U.S. Department of Health and Human Services (HHS) withstood a DDoS attack consisting of millions of hits in a several hour period."[10] In Paris, a DDoS attack resulted in 44 hospitals being inaccessible to remote workers for several hours[11] and in Australia thousands of people lost access to a government online portal used to access welfare services.[12]

Such evolving threats can be effectively addressed by equally dynamic and flexible solutions, rather than prescriptive, compliance-focused regulatory requirements. Collaboration between government and all relevant industry sectors also is key to counter the significant sophistication of these new types of attacks.

THE NEED TO PREVENT RANSOMWARE

Whilst malign actors can choose from multitudes of cyberattack vectors, ransomware has dominated the last 24 months, and in 2021 has reached the top of both business and political agendas. For example, in response to cybersecurity concerns, including those related to ransomware, the United States announced that it would "bring together 30 countries to accelerate our cooperation in combating cybercrime."

Ransomware is one of the most pervasive threats[1] facing our businesses, critical infrastructure providers, supply chains, schools, hospitals, governments and communities. On-average there is one ransomware attack on businesses every 11 seconds. Every 40 seconds, one of those attacks proves to be successful[2] and no attack is the same.[3] There is also a growth in ransomware demands (the largest to date occurred in 2021 and stood at $70 million).

Crucially, once a victim is hit by ransomware, there is little that can be done. In 2021, the average pay-out by a mid-sized organisation that fell prey to a ransomware attack was $170 404 with a total average cost to recover from a ransomware attack at $1.85 million.[4] As Lindy Cameron, CEO of the UK's National Cyber Security Centre noted recently "turning up to a ransomware incident [...] feels like the fire service turning up to a house that has already burned down. There might be some forensic evidence that the police might pursue[...] But these groups know what they're doing, and that hardly ever happens. Often, it's a case of rebuilding from scratch." [5]

[1] WSJ, FBI Director Compares Ransomware Challenge to 9/11, 2021

[2] Blackberry, White Paper Ransomware Prevention, 2021

[3] Sophos, Relentless REvil, revealed: RaaS as variable as the criminals who use it, 2021

[4] Sophos, State of Ransomware Report, 2021

[5] UK NCSC, 2021

[9] CSDE, International Botnet and IoT Security Guide 2021.

[10] Id.

[11] Id.

[12] Id.

Compounding an already daunting situation, threat actors are leveraging the growing complexity of the cyber domain as an opportunity to conduct offensive operations with almost complete deniability. This ability to operate in increasing obscurity is encouraging a growth in more destructive cyberattacks—incidents are proving to be more costly at a staggering $4.24 million per incident on average in 2021, a 10% year on year increase. Malware such as Wiper (designed to wipe an entire hard drive), the growth in multifaceted attacks (such as a ransomware attack followed by a DDoS attack), and data leakage to force payment are all indicative of increasingly confident cyber adversaries.

This confluence of effects comes at a time when almost 4 million cybersecurity jobs are unfilled globally[13] and cyber insurance rates are soaring by up to 40%[14]. These mounting vulnerabilities and consequences create an exceedingly unhospitable landscape for businesses. The impact of cyberattacks on businesses and individuals has become so pervasive that cyber risk is now a top concern[15] of CEOs globally. State-sponsored operations like the 2020 SolarWinds hack, the 2021 attack on the Microsoft Exchange Server, and the growing list of non-state cyber incidents are starkly visible warnings of the urgent need to protect businesses, communities, and economies from malicious cyber activities.

The proliferation of OCC and the level of access to OCC threaten to further destabilise relations between states. As the complex cyber environment provides a cloak of deniability and obscurity, the line between nation state and criminal type activity is blurred. Sophisticated attacks are no longer the preserve of nation states. Traditional international behavioural norms could be undermined as nation states attempt to combat the occurrence and mitigate the impact of cyber activity. Unintended victims will also be impacted, for example, the NotPetya attack in 2017, designed to impact Ukrainian targets, quickly spread across the globe, impacting multiple companies, and costing over $10 billion globally. The concept of collateral damage will likely become an increasingly used term as cyberattacks go beyond their initial target due to the level of connectivity globally. This will ultimately create further confusion, allowing cyber threat actors to conduct more reckless attacks amid a "fog of war".

It is important here to introduce the concept of societal security, since it is no longer only the concern of information security and cybersecurity "internally" in the organisation, but also to understand the impact that a cybersecurity incident can have on the society depending on the activity carried out by the victim organisation. Proliferation is compounded by the lack of clear and effective legal and policy counter measures against malicious actors, particularly at the nation state and international level, combined with the lack of knowledge that judges and other actors of the justice administration organisations have on cybersecurity issues. Due to the vast international nature of the internet, there are many states without the ability, or without the appetite, to impose regulatory measures. With a general easing of the "barrier of entry" to OCC, particularly with the "Access as a Service" (AaaS) model, the cyber domain is likely to become more unstable and risky. As seen with other global security threats, legal and policy measures alone are not sufficient government activities to stem the tide—strong international government cooperation, public-private voluntary collaboration, and deterrent and punitive measures against cyber criminals and nation-state sponsors are an imperative.

[13] HDI, The cybersecurity skills gap, 2020

[14] Reuters, Cyber reinsurance rates rocket, 2021

[15] PWC, CEO Survey, 2021

PART 2: Cybersecurity risks' indirect economic and social impacts

Cyberattacks destroy economic opportunity, stifle economic growth and are responsible for substantial job losses across all economies. An estimated 60% of small companies go out of business after a cyberattack[16]. A recent report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, cites the cost of cybercrime at €5.5 trillion, up from €2.7 trillion in 2015.[17] As the type and diversity of cyberattacks increase, businesses are increasingly recognising the monetary impact of both direct as well as indirect economic costs, so the €5.5 trillion estimate is likely to further increase over time. Should this trend remain unaddressed, we can reasonably expect another doubling of this cost to EUR 11 trillion by 2030, corresponding to the combined nominal GDP of Germany, France and Japan.

Cyber incidents can potentially lead to several different types of losses, including damages to tangible and intangible assets, losses related to business disruption and theft, as well as various forms of liability to customers (including governments), suppliers, employees, shareholders and society at large.[18] It is estimated that the direct costs associated with intellectual property (IP) theft and financial crime account for two thirds of current monetary losses. Intellectual property theft causes businesses billions of dollars a year and robs nations of the economic security provided by jobs and tax revenues[19]. Additional indirect costs associated with these crimes are increasingly being captured and recognised.[20] A 2020 report based on a survey of over 1500 companies noted the following examples of indirect costs to organisations impacted by cybercrime:[21]

1. **System downtime**: Downtime is a common experience for around two thirds of respondents' organisations. The average cost to organisations from their *longest* amount of downtime in 2019 was $762,231. 33% of survey respondents stated IT security incidents resulting in system downtime cost them between $100,000 and $500,000. Depending on the industry, system downtime also results in downtime for dependent or interdependent organisations, and often these downtimes include those for critical and government-provided services.
2. **Reduced efficiency**: As a result of system downtime, organisations lost, on average, nine working hours a week leading to reduced efficiency. The average interruption to operations was 18 hours. Reduced efficiency may result in disruption or reduction of critical products and services.
3. **Incident response costs**: According to the report, it took an average of 19 hours for most organisations to move from the discovery of an incident to remediation. Many security incidents can be managed in-house, but major incidents can often require outside support with high rates that form a significant portion of the cost of a large-scale incident.
4. **Brand and reputation damage**: The cost of rehabilitating the external image of the brand, working with outside consultancies to mitigate brand damage, or hiring new employees to prevent against future incidents is part of the cost of cybercrime. 26% of the respondents identified damage to their brand from the downtime they experienced because of a cyberattack. In this era of distrust[22], where institutions are already facing steep declines in trust, brand and reputation damage can be difficult or even impossible to recover from.

[16] US SEC, The Need for Greater Focus on the Cybersecurity Challenges Facing SMEs, 2015

[17] European Commission, JRC Publications Repository - Cybersecurity, our digital anchor (europa.eu), 2021

[18] OECD, Enhancing the Role of Insurance in Cyber Risk Management, Chapter 2 Types of Cyber Incidents and Losses, 2017

[19] U.S. Federal Bureau of Investigation, Intellectual Property Theft/Piracy, 2021

[20] McAfee, The Hidden Costs of Cybercrime, 2020

[21] McAfee, The Hidden Costs of Cybercrime, 2020

[22] Forbes, In An Era of Distrust, Here Are Three Ways To Transform Your Organization, 2018

Looking beyond monetary losses, the social impact of cyberattacks, though harder to detect and quantify, is no less significant. In many ways, it can be more insidious and far-reaching as it drives behaviours which compound the impact of all other factors over time and cannot always be detected immediately or measured statistically. The social impact of cyberthreats manifests itself in three principal, inter-related dimensions of behaviour: (i) the psychological reactions of individuals, (ii) the change in organisational behaviours, and (iii) the non-monetary, real-world effects on large segments of society.

1. **The psychological reactions of individuals: disengagement with the private and public sector**—The psychological effect of cyberthreats on individuals, both potential and actual victims, can lead to anxiety, worry, anger, outrage, and depression resulting in a cynicism toward, withdrawal from or a reluctance to engage with digital technologies and wider technological innovation, and even to undertake cyberattacks as retaliation measures. A recent report concerning COVID-19 affected attitudes toward technology notes that two out of three Americans expressed concern that their information would be breached during the 2020 holiday season.[23] A report based on survey responses from 3,264 consumers in the United States, United Kingdom, France and Germany noted a quarter of consumers said they would completely stop engaging with a brand that experienced a breach. [24] 78% of respondents would stop engaging with a brand online and more than one third (36%) would stop engaging altogether if the brand had experienced a breach. Nearly half (49%) would not sign up and use an online service or application that recently experienced a data breach. Almost half (47%) have made changes to the way they secure their personal data because of recent breaches and over half (54%) are more concerned with protecting their personal information today than they were a year ago.[25] As businesses (and governments) increasingly provide goods and services via online channels and rely on cyber-physical connection to enable public services, the long shadow of cyber threats may dissuade many individuals from engaging with private and public sector entities.
2. **The change in organisational behaviours: increased costs and/or decreased online operations**—In recent years, organiations of all shapes and sizes have become profoundly aware of the potential negative impacts of cyberattacks and approach cybersecurity as an existential concern. In addition to the obvious monetary and proprietary losses, loss on business continuity, as well as legal exposure and regulatory sanctions, organisations recognise the potential damage to their reputation and the loss of trust from customers and business partners in the supply chain, which result in declining sales and profits. A recent study reviewed 40 data breaches at 34 companies listed on the New York Stock Exchange and found that the share prices of compromised companies fell an average of 3.5% following an attack.[26] Though the degree of cybersecurity preparedness varies broadly across industry sectors and organisational, investments and improvements are on a growth trend. Many organisations have changed how they collect and store information to ensure that sensitive information is not vulnerable. Customers are also more interested in knowing how the businesses they deal with handle security issues, and they are more likely to choose businesses that are up front and vocal about the protections they have in place. We should expect to see these trends in transparency and trust-building between business and consumer to continue to increase in the near future.

[23] Generali Global Assistance, 2 in 3 Concerned About Data Breaches During The Holiday Shopping Season This Year, 2020

[24] Verizon, Why is the social impact of cyber security important to business?, 2020

[25] Ibid.

[26] Comparitech, How data breaches affect stock market share prices, 2021

However, not all organisations have the same adaption capacities, and efforts to mitigate cyber risks have led to specific business practices that preclude companies from reaping the full benefits of going digital. For example, some companies have chosen to shut down or scale down their online stores out of concern that they cannot adequately protect themselves from cyberattacks. These trends (i.e., investment in new tools and skills, or withdrawal from online operations) will continue to incur significant costs or lost opportunities for businesses, and unfortunately, will often prove insufficient to ward off increasingly multifarious and sophisticated cyber threats.

3. **The non-monetary, real-world effects on large segments of society: impact on public health and safety**—In addition to the economic impacts of large-scale cybercrime discussed above, there are other effects which, though not necessarily measured in monetary terms, greatly influence society by disrupting the normal activities of life. In addition to the well-known incidents of recent months, such as SolarWinds, Microsoft Exchange Server and the Colonial Pipeline, which had consequences such as compromising data, preventing system access, or causing shocks to the energy supply chain, more localised events have demonstrated the paralysing effects of cyberattacks, regardless of scale. In 2019, 22 towns in Texas sharing a software vendor were the target of a ransomware attack. The malicious actors asked for a ransom of $2.5 million for the restoration of administrative services, and residents of these towns could not access records or pay utility bills while under siege.[27] On 10 September 2020, the University Hospital Düsseldorf (UHD) experienced a cyberattack that led to gradually failing systems and data access, forcing the hospital to de-register from providing emergency care and incoming patients being diverted to other hospitals. The incident made headlines globally, as a woman who needed urgent admission had to be sent to another facility roughly 30 km away. This resulted in her treatment being delayed and contributed to her death. It would take the hospital almost two weeks to restore essential services and allow emergency care to re-open, and many more weeks to become fully operational again.[28]

The trends described above make it clear that while business investment in prevention and defensive capabilities is essential, the private sector alone is unable to deter, prevent, or properly shield itself (and the communities it helps sustain) from the destructive effects of cyberattacks. Cybersecurity is a shared responsibility between the private and public sectors, and both must work together to curb threats and mitigate risks. The private sector and by extension our economies will continue to bear the brunt of these attacks. Business therefore urges governments to take more assertive and ambitious action to curtail cybersecurity threats that impact individuals, communities, and economies. The following section sets out the necessary actions that governments must take to lessen the prevalence, proliferation, and consequences of cyberthreats and build a more secure cyberspace for communities to thrive.

[27] Verizon, Why is the social impact of cyber security important to business?, 2020

[28] University of Hamburg, The Düsseldorf Cyber Incident, 2020

PART 3: Call for governments to fully implement international and national instruments and for ambitious and concrete actions

1. **Governments must uphold commitments to international law and norms of responsible state behaviour in cyberspace**: In 2021, the United Nations (UN) Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE) on cybersecurity adopted two reports that outlined expectations for nation-state behaviour in cyberspace.[29] [30] These recent frameworks build upon previous agreements, such as the 2015 GGE report[31], as well as other bilateral and multilateral commitments in this space.

   Amid a flood of disruptive and damaging cyberattacks around the world, this development is welcome, as it comes after several years of states unable to come together to address these critical challenges. The time has come to implement these norms and ensure effective compliance and holding non-compliant states accountable. A potentially useful tool is the survey of norms implementation[32] proposed by Australia, Mexico and other states that encourages governments to assess and report on how they are implementing their commitments.

2. **Governments must bolster cross-border cooperation to effectively tackle cybercrime**: A globally coordinated approach to sharing information and cooperation and tackling cybercrime is essential. Cyber criminals are not confined to national borders and they understand the existing legal grey zones, yet legislative and regulatory powers only apply to defined jurisdictions such as a nation or region. This makes it all the more important for law enforcement to have the ability to share information and collaborate to bring them to justice, with appropriate safeguards, and full commitment of the jurisdictions used by criminals for their criminal actions. The Budapest Convention creates a framework to support this exchange of information, however states need to ensure its execution is well resourced and supported domestically. We call upon states who have not yet joined the Convention to do so.

   The UN OEWG and GGE are complementary to existing commitments on curbing cybercrime, such as those enshrined in the Budapest Convention on Cybercrime[33]. In addition to upholding their commitments under the Budapest Convention, governments must further engage in a coordinated, multilateral approach to combat the ever-growing risk of ransomware and other cyberattacks. In June 2021 at the G7 Summit[34], leaders pledged to take steps to improve online safety, advance a common view of existing international law application to cyberspace, and identify and disrupt ransomware criminal networks. Also in June 2021, at a meeting of the North Atlantic Council in Brussels, 30 NATO allies[35] announced a Comprehensive Cyber Defence Policy which includes using NATO as a platform for information sharing and engagement on international cybersecurity concerns and improving the collective ability to defend against threats from state and non-state actors against networks and other critical infrastructure. In October, these same messages were reinforced in a White House hosted Summit on Ransomware.[36]

[29] UN, GGE Report 2021

[30] UN, OEWG Report 2021

[31] UN, GGE Report 2015

[32] DFAT, Joint OEWG Proposal, 2020

[33] Council of Europe, Budapest Convention, 2001

[34] G7, Joint Actions on Forced Labor in Global Supply Chains, Anticorruption, and Ransomware, 2021

[35] NATO, Brussels Summit Communiqué, 2021

[36] White House, Background Press Call on the Virtual Counter-Ransomware Initiative Meeting, 2021

In addition, governments have looked to the OECD's 2015 Recommendation on Digital Security Risk Management for Economic and Society Prosperity—also known as the 2015 Security Guidelines—for guidance on general principles to inform the foundation of domestic security programs as well as operational principles to guide program implementation. This commonality is aimed at enabling like-minded international collaboration to improve preparedness.[37]

Governments must now act on implementing these commitments by investing in our collective security. and prioritising prevention-first approaches to countering cyberthreats.[38] Nefarious actors will strike wherever there is a vulnerability, security gap and/or an incentive. As such, a united front among leading nations will be critical to bolstering global cyber defences. An important aspect of this could be highlighting norms violations, which supports the need to strengthen and improve the articulation of international agreements on the matter. The attribution of a cyberattack to a state that is in violation of international norms should always include an explicit and direct articulation of which norm was transgressed and how. Where reasonable, greater transparency in the underlying information used in drawing those conclusions will lend the attribution greater credibility and further strengthen the recognition of norms.

3. **Governments must implement and enforce legal instruments that deter malicious cyber activity**: National legal regimes must provide states with the tools necessary to effectively combat cyber threats and protect their businesses and communities from an ever-growing ecosystem of affiliated and unaffiliated threat actors with both political and criminal objectives. Turning the tide against escalating cyber conflict will require states to go beyond high-level commitments and focus on their implementation within individual national contexts, going as far as ensuring that malicious criminal actors that break the rules are held accountable. Implementation efforts should also include formal activities to develop managerial and technical skills and competences in judicial, security, and legislative actors involved in the investigation and administration of justice and set up the organisational infrastructure that's required to implement international obligations and best practices. This requires resourcing—for example 20% of countries do not have modern cybercrime legislation[39] and about half do not have a national Computer Incident Response Team (CIRT/CSIRT). Governments should recommit themselves to ensuring the resources are available so that all countries are in a position to cooperate with each other and industry to implement to take the actions required.

The work at the UN so far has laid an invaluable foundation by establishing and reinforcing norms for responsible state behaviour online, such as the 11 norms adopted in the 2015 UN GGE, but the dialogue cannot stop here. Going forward, we need to work together as a global community to ensure that malicious actors are held accountable. If lines are crossed, norms broken and international laws violated, there should be consequences. Undermining the security of Information and Communication Technology (ICT) supply chains, attacking healthcare organisations, threatening energy transportation, and jeopardizing food resources cannot become the kinds of activities that are normalised due to inaction.

[37] The OECD's 2015 Recommendation on Digital Security Risk Management for Economic and Society Prosperity, includes General Principles (awareness, skills and empowerment; responsibility; human rights and fundamental values; co-operation) as well as Operational Principles (risk assessment and treatment cycle; security measures; innovation; preparedness and continuity).

[38] BlackBerry, From Aspiration to Realization: The Evolution of the Prevention First Approach to Security, 2021

[39] According to UNCTAD's Global Cyberlaw Tracker, at https://unctad.org/page/cybercrime-legislation-worldwide.

4. **Governments must curtail the proliferation of offensive cyber tools, instruments and cyberweapons**: Counter proliferation policy options in cyberspace are underutilised. As offensive cyber capabilities continue to proliferate with increasing complexity and to new types of actors, the imperative to slow and counter their spread only strengthens. But to confront this growing challenge, international policymakers must understand the processes and incentives behind it. The issue of cyber capability proliferation has often been presented as attempted export control on intrusion software, creating a singular emphasis on malware components, diverting attention from other phenomena and applicable controls in terms of security and cybersecurity. There is an urgency to develop international and coordinated national policy tools that aim to curtail the proliferation of OCC.

   There is an urgent need for governments to more broadly understand cyber proliferation as the proliferation of multiple capabilities. This would give policymakers enough granularity to craft feasible counterproliferation policies. Understanding the way that criminal markets, governmental agencies, and private Access as a Service (AaaS)[40] groups offer and build state-of-the-art products for conducting offensive cyber operations also allows policymakers to target a specific subset of actors without damaging the cybersecurity industry as a whole. Specifically, uncovering the role of semi-regulated, or self-regulated, and criminal AaaS groups play in proliferating offensive cyber capabilities will help drive more effective counterproliferation policy, such as "know your vendor" laws or regulations, and development of ban lists for vendors caught selling capabilities to states or entities on published lists of concern. Similarly, malware-as-a-service and surveillance-as-a-service underground market proliferate cyber tools and capabilities which threatens online ecosystems, targeting citizens, journalists and government officials alike, at an increasing pace, and government intervention of these proliferation is urgently needed.

5. **Governments must adopt a multistakeholder approach to inform policies and protect critical infrastructure**: States should also view the UN developments and efforts by OECD member nations mentioned above, as a call to action—with the recognition that they cannot do it alone. While governments have unique responsibilities in implementing these agreements and protecting business and civil society from foreign and domestic cyberthreats, the shared nature of cyberspace requires collaboration between and across stakeholder groups to protect the safety and integrity of cyberspace. Multistakeholder action is critical across rules development, capacity building, and implementation.
   For example, business provided invaluable technical expertise to the experts group that developed the 2015 OECD Security Guidelines to ensure that the framework is commercially and technically feasible. In the same vein, the Global Forum for Cyber Expertise (GFCE) can act as a resource for states, coordinating regional and global cyber capacity projects and initiatives; sharing knowledge and expertise by recommending tools and publications; and matching individual needs for defensive cyber capacities to offers of support from the community. On the other hand, the important collection of technical standards and good practices provided by ISO, ISA, IEC, NIST, among others, are fundamental technical resources for an adequate development of information security, cybersecurity and privacy management systems.

[40] Here we refer to AaaS groups as ones that offer various forms of "access" to target data or systems, thus creating and selling OCC at an alarming rate. These groups advertise their wares to actors who would not otherwise be able to develop such capabilities themselves. AaaS products and services may vary in form, but share foundations that can be categorized under: Vulnerability Research and Exploitation, Malware Payload Development, Technical Command and Control, Operational Management, and Training and Support.

The ICT infrastructure is largely built and maintained by the private sector, so deliberations on peace and security in cyberspace need to be inclusive of non-governmental voices. The above-mentioned UN reports also highlight the need to protect critical infrastructure. With that in mind, states should prioritise these essential sectors for their cybersecurity investments and leverage globally accepted voluntary standards and practices to create their national cybersecurity frameworks. This will ensure that they create a consistent baseline for international cooperation and a clear point of reference for improvement and innovation over time. Expressly recognising these sectors as needing protection will drive greater investments in their security, but it should also be seen as a red line for malicious behaviour, which—when crossed—will trigger consequences.

The joint proposal by delegates of Egypt and France at the OEWG for the establishment of a Programme of Action for advancing responsible State behaviour in cyberspace is a promising way forward for establishing a UN forum to consider the use of ICTs by states in the context of international security and to ensure that the multistakeholder practices implemented by the OEWG so far continue to be part of all UN work in this area.

ROLE OF BUSINESS AND SHARED COLLABORATION

While actions by governments must be taken to minimise risks, industry also needs to ensure preventive actions. In particular, given the focus of this document, the security of the software supply chain and critical infrastructure protection are of strategic and economic importance.

Improve the security of software and information systems supply chains. The software supply chain involves a complex web of dependencies with numerous third-party developers and components. In many cases users of ICT systems have little knowledge of the software components that are embedded in their control systems. The pervasiveness of open-source software is one compelling reason why this is so critical. By some accounts, the average software application depends on more than 500 open source libraries[41] and components. Experts indicate that more than 90%[42] of commercial applications contain outdated or abandoned open source components. Constant updating is precisely one of the means to counteract vulnerabilities potentially present in the software. Governments and software developers should collaborate to increase the transparency and security of the software supply chain for critical infrastructure and devices. This means adopting a secure software development life-cycle approach to mitigate software supply chain risk; leveraging best-in-breed technology to undertake software composition analysis that can produce a software bill of materials, and implementing AI-driven endpoint security tools that have been proven to prevent ransomware and malware from deploying.

While doing so, governments need to ensure that software developers' intellectual property and trade secrets are protected and that source code disclosure of proprietary software is not mandated. Timely vulnerability disclosure by software developers must ensure principles of responsible and coordinated disclosure such as the CERT® Guide to Coordinated Vulnerability Disclosure.[43] This will help developers, manufacturers, and critical infrastructure operators monitor software components for vulnerabilities, manage supply chain risks, and decommission products that have a history of security, performance, or reliability issues. Timely and appropriate incident reporting, if carefully crafted, has the potential to be a helpful policy lever.[44]

[41] Synopsis, Open Source Security and Risk Analysis Report, 2021

[42] Synopsis, Open Source Security and Risk Analysis Report, 2020

[43] Carnegie Mellon University Software Engineering Institute, The CERT Guide to Coordinated Vulnerability Disclosure, 2019

[44] Information Technology Industry Council, Policy Principles for Security Incident Reporting in the U.S., 2021

Improve the security of critical infrastructure through dedicated security frameworks that emphasize prevention-first approaches. For instance, the National Institute of Standards and Technology (NIST) created a Cybersecurity Framework[45] to improve critical infrastructure cybersecurity for the U.S. government and the private sector. This voluntary framework was created based on existing standards, guidelines, and practices for organisation to better manage and reduce cybersecurity risk. The NIST Cybersecurity Framework is composed of three main components: Framework Core, Implementation Tiers, and Framework Profiles. The Framework Core has five functions: Identify, Protect, Detect, Respond, and Recover which can be used in conjunction with those defined in the family of standards ISO/IEC 27035 and BS 11200. The Framework Core enables effective communication between multi-disciplinary teams. The purpose of the Framework Implementation Tiers is to ensure that cybersecurity risk decisions meet organisational goals and are feasible to implement. The Framework Profiles are intended to create alignment of organisational requirements, risk appetite, and resources to desired outcomes identified in the Framework Core. These three framework components work together in an effort to achieve cyber resiliency by aligning cyber risk management and increase information sharing between the government and private sectors.

CONCLUSION

The destructive effects of cyberattacks have reached dramatic proportions and will continue to worsen failing bold and decisive, globally coordinated action from governments and the broader multistakeholder community. Businesses and the communities they help sustain are in dire need of effective remedies that will mitigate cybersecurity risks and lessen the impact of cyberattacks. The aggregation of economic and social costs, coupled with the increasing volume of cyberthreats has led to a positive trend towards long overdue, focus on cybersecurity by governments, yet this is still critically insufficient.

Governments are primarily responsible to protect their citizens from foreign and domestic, affiliated and unaffiliated threat actors with both political and criminal objectives, which also applies in cyberspace. Decisive action from governments to styme cyber threats and broad multistakeholder collaboration will help bolster economic confidence, prevent disruptions in global trade, and ensure a more secure cyber environment where businesses and communities can thrive.

Crucially, increased government action must be based on broad multistakeholder dialogue so as to fully understand the issues, find an appropriate balance and not hamper entrepreneurialism and innovation. Governments must also seek to harmonise and align to the greatest degree possible any actions taken to effectively address these evolving issues.

This document has raised the urgency of government action under five areas that can, if implemented, help make tangible progress. It also noted the necessity of private-public collaboration and the crucial role of the private sector to continuously invest in the security of technologies and supply chains. Subsequent papers will provide further detail and guidance on concrete actions to be taken by governments, as well as highlight current and recommended initiatives from the private sector, focusing especially on the implementation of international norms, the reduction of cybercrime, and the protection of critical infrastructure.

[45] US NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2018

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 100 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

www.iccwbo.org   Follow us on Twitter: @iccwbo