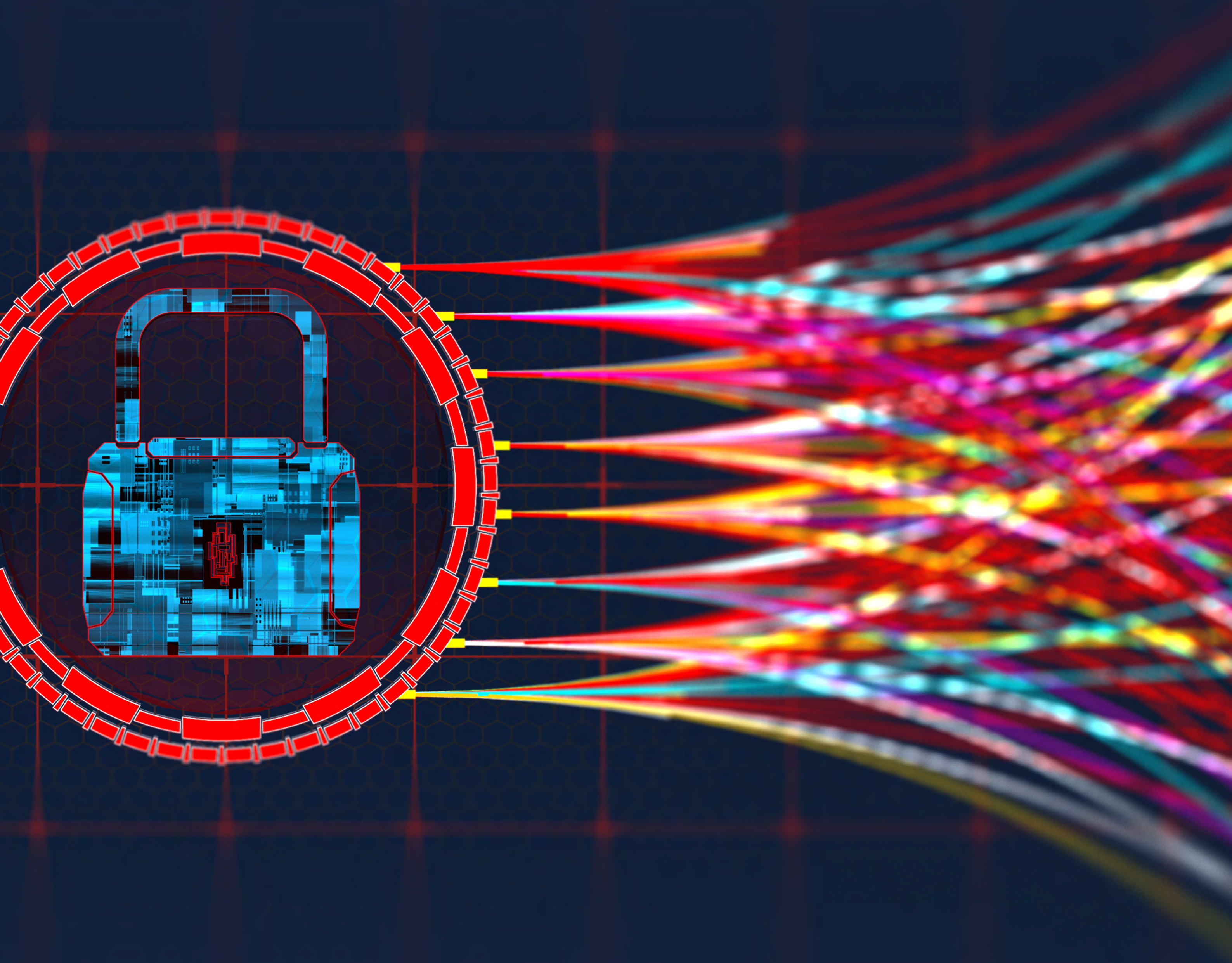
Shaping the Future of
Cybersecurity and Digital Trust

Partnership against Cybercrime

INSIGHT REPORT

NOVEMBER 2020



Cover: By Valery Brozhinsky, Getty Images

Inside: Getty Images

Contents

Preface

This report presents the recommendations of the Partnership against Cybercrime Working Group as a first step towards establishing a global architecture for cooperation.

Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance, USA; Special Assistant to the US President and Cybersecurity Coordinator for the US Government (2012-2017)

Tal Goldstein
Head of Strategy, Centre for Cybersecurity, World Economic Forum

Amy Hogan-Burney
General Manager, Digital Crimes Unit; Associate General Counsel, Microsoft, USA

Derek Manky
Chief, Security Insights and Global Threat Alliances, Fortinet, USA

Cybercrime is a global threat that should concern every decision-maker, whether at the corporate or national level. According to the World Economic Forum *Global Risks Report 2020*, over the next 10 years, cyberattacks will be the second greatest risk businesses will face.[1] While nation state cyber activities tend to garner the most international attention, cybercriminals are responsible for the majority of malicious activity on the internet – cybercrime is estimated at about 80%.[2] As a result, reducing cyber risk means reducing and mitigating cybercrime.

Traditionally, governments have been responsible for combating crime. However, the unique realm of cyberspace has proved that governments do not and will not have all the capabilities needed to combat the cybercrime threat alone. In fact, many of the required capabilities reside in the private sector, such that private companies must be part of the solution. Enabling stronger operational collaboration between the private and public sectors at the global level and combining their resources and capabilities are therefore crucial elements in reducing the risk posed by cybercrime. Various significant collaborative initiatives exist, but they remain fragmented and insufficient for current needs. A paradigm shift in the way we collectively address this challenge is thus required.

The World Economic Forum created the Partnership against Cybercrime initiative to address this global challenge by exploring ways to amplify public-private cooperation against cybercrime and overcome existing barriers to cooperation. The initiative brought together key private and public stakeholders, including leading law enforcement agencies, international organizations, cybersecurity companies, service and platform providers, global corporations and leading not-for-profit alliances.

Despite the challenges of the passing year due to the COVID-19 pandemic, the community showed notable commitment to the task, driven by the mutual interests and benefits of working together towards a shared goal. The members of the World Economic Forum Partnership against Cybercrime Working Group engaged in a series of virtual yet intense discussions that resulted in the three main recommendations presented in this report. The approach chosen for this initiative was not only to understand the challenges, but to design forward-looking and action-oriented solutions.

The first two sections of this report present the challenge of cybercrime and the need to foster public-private cooperation. The third and fourth sections lay out the principles and considerations formulated by the working group to support collaborative action against cybercrime. The final section outlines a potential global architecture to increase existing efforts and facilitate the required cooperation.

This report highlights the commitment of an engaged, purpose-driven multistakeholder community that continues to develop and implement these concepts with the aim of reducing cybercrime globally. We hope it will encourage other like-minded individuals and organizations to join us in advancing this critical mission.

Foreword

A public-private partnership against cybercrime is the only way to gain an edge over cybercriminals. This report provides key insights on how to achieve this together.

Jürgen Stock
Secretary-General
International Criminal Police Organization (INTERPOL), Lyon

Of all the types of crime, cybercrime continues to increase at the fastest rate. According to INTERPOL's recent assessment of the global cyberthreat landscape,[3] cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social, economic and health situation around the world.

While crimes such as burglary and assault are more visible, cybercrime is largely hidden, leading many people to underestimate its actual damage or the likelihood of becoming a victim. But the effects of cybercrime can be just as devastating as physical crimes, impacting numerous individuals and organizations everywhere.

To address this threat, we must create barriers to entry, such as raising the cost of engaging in criminal activities and the overall risk for cybercriminals. Law enforcement agencies worldwide are actively investigating cybercrimes with the aim of prosecuting cybercriminals. INTERPOL, through its Global Cybercrime Programme, is facilitating law enforcement cooperation and promoting police capacities in the field of cyber. But this is not enough.

Against cybercrime, the solution can only come from public-private cooperation. The private sector plays a fundamental role in the ability to understand and act against cybercriminals. Only by ensuring that leading companies work side by side with law enforcement can we effectively respond to the cybercrime threat.

The World Economic Forum is well positioned to promote this cooperation. With INTERPOL and other primary stakeholders from the private and public sectors, it has devised the recommendations presented in this report. Implementing them and continuing to work together through the Partnership against Cybercrime will drive momentum to amplify collaboration in our joint fight against cybercrime.

Executive summary

The public and private sectors must work together to fight cybercrime. To do so, each needs to embrace effective ways of working together and foster needed alliances.

Cybercrime impacts everyone, from individuals to global corporations and critical infrastructures or governments. It causes immense, though not always visible, damage to economies and societies. It drastically undermines the benefits of the Fourth Industrial Revolution, increases inequality and hinders international cyber stability efforts.

As in the case of any other crime, systematic containment efforts against cybercrime must also include actions against the sources of the threat. This can only be achieved through stronger operational collaboration between the private and public sectors, leveraging private companies' unique position and capabilities in this field. While various significant collaborative initiatives exist, they remain fragmented and insufficient for current needs and an ever-evolving cybercrime threat landscape.

Following the 2016 work on Recommendations for Public-Private Partnership against Cybercrime, the World Economic Forum's Partnership against Cybercrime initiative was launched in January 2020 to explore ways to amplify public-private collaboration in cybercrime investigations and initiate a paradigm shift in the way to collectively deal with the growing impact of cybercrime. The initiative's working group included more than 50 representatives from leading public and private organizations.

This report presents the recommendations of the Partnership against Cybercrime Working Group in three areas:

Promoting principles for public-private cooperation to combat cybercrime
The working group defined six principles, to be endorsed by both law enforcement and private companies, which can enable sustainable, repeatable and effective cooperation:

- Embracing a shared narrative for collective action against cybercrime
- Cooperating on the basis of long-term strategic alignment
- Undertaking trust-building behaviours
- Systematizing cooperation
- Ensuring value for participation in the cooperation
- Respecting concerns and challenges

Taking collaborative action to disrupt cybercrime ecosystems
The working group also emphasized the need to explore the full spectrum of possible courses of action to raise the costs and risk for cybercriminals, leveraging the respective expertise and capabilities of both the public and private sectors. Specifically, potential coordinated measures to disrupt and dismantle criminal activities at scale are insufficiently used. A decision to participate in such operations should not be made lightly, but organizations should not be paralysed by inaction. The Group highlighted key considerations for decision-makers in assessing these actions, to maximize the likelihood of success and minimize unnecessary risks.

Partnering to combat global cybercrime
To increase existing efforts and fully harness the power of the private sector, facilitating sustainable and effective cooperation, the working group **recommends launching a three-level system** comprised of:

- **A global partnership**, building on the existing Forum initiative, to bring together international stakeholders to provide an overarching narrative and commitment to cooperate; foster interaction within a global network of entities that drive efforts to fight cybercrime; and facilitate strategic dialogues and processes aiming to support cooperation and overcome barriers in the long term.
- **Permanent Nodes**, a global network of existing organizations that strive to facilitate public-private cooperation over time.
- **Threat Focus Cells**, short-term, mission-driven groups of partners that engage in concrete, operational, cooperative efforts. These cells will be hosted and maintained by the Permanent Nodes.

1 The global challenge of cybercrime

1.1 The impact of cybercrime

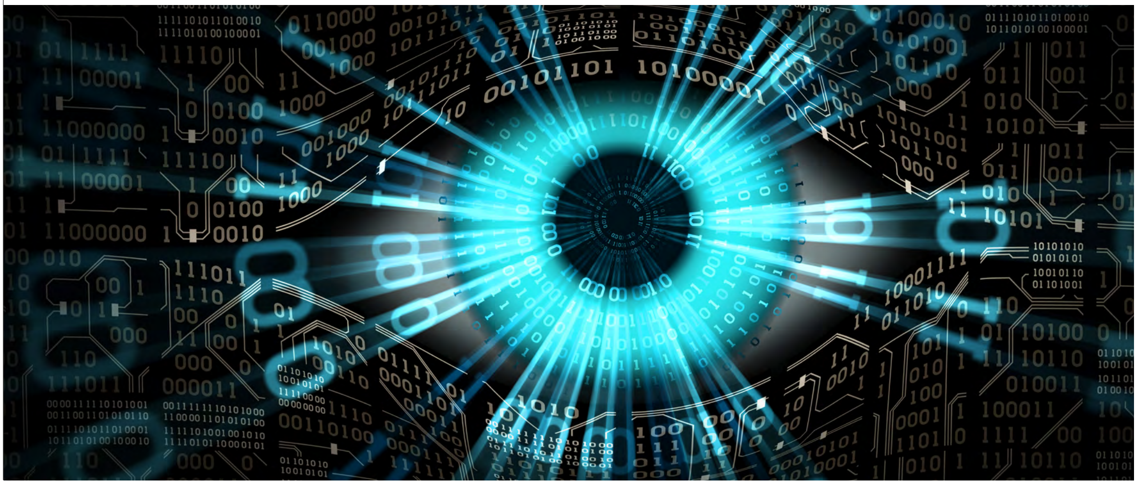
An estimated 4.66 billion people around the world currently use the internet,[4] a number that has tripled in the past 12 years as connectivity has become more accessible, and that will continue to increase. Our reliance on the use of computers and technology has changed the way we conduct business, communicate and socialize, and technology is an indispensable part of all facets of life.

Humans are increasingly dependent on the internet, yet our efforts to protect people, data, devices and the infrastructure of the internet itself from cybercriminals have not matched the threat they pose. Cyber criminals steal an estimated $600 billion per year from governments, companies and individuals,[5] while the overall loss of company revenues over the course of five years, from 2019 to 2023, will reach $5.2 trillion.[6] In fact, cybercrime is one of the most disruptive and economically damaging criminal activities. Not only does it cause substantial financial damages and pose a serious threat to society and the global economy, it also has indirect effects in undermining the public's confidence in digital transformation and overall trust in technology.

Our connected world has become a lucrative playground for cybercriminals who can launch attacks on victims in multiple countries and jurisdictions with little fear of being caught. They use malicious software programs and technical infrastructure to steal funds, intellectual property and sensitive personal information. They carry out attacks on individual users, networks and corporate systems to engage in an enormous amount of fraudulent and destructive activity. The tools and services available to criminals as part of the crime-as-a-service model, which lowers the entry barrier to committing cybercrime and provides relatively sophisticated cyber capabilities to almost anyone who is willing to pay, are also significantly increasing the growing impact of cybercrimes.

The cybercrime threat landscape is quite diverse and dynamic. Threat actors range from individuals, to loosely connected cross-national collectives, to large organizations that in many cases enjoy a degree of support, tolerance or even direction from nation states. Cybercriminals abuse encryption, cryptocurrencies, anonymity services and other technologies. Financially motivated cybercriminals constantly innovate to increase their profits. In addition to financial crimes, criminals use internet-based infrastructure to uphold terrorism and drug trafficking, and spread disinformation to destabilize governments and democracies.[7]

At the macro level, cybercrime is an enormous barrier to digital trust, greatly undermining the benefits of cyberspace and hindering international cyber stability efforts. In addition, cybercrimes increase global inequality, putting both the corporations and governments with fewer resources at higher risk of falling prey to these activities. Developing countries with weak legal and enforcement regimes as well as inadequate capacity to mitigate cyberthreats are particularly exposed to these crimes. If not mitigated, cybercrimes could undermine these countries' efforts to formalize their economies using digital technologies, negatively impacting the anticipated digital dividends.



BOX 1

Cybercrime and COVID-19

Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation caused by COVID-19 around the world. At the same time, the higher dependency on connectivity and digital infrastructure due to the need for physical distancing further expands the avenues of cyber intrusion and attack.

To maximize their financial gain and intended damage, cybercriminals are shifting gears to target businesses, governments and critical infrastructure that play a crucial role in responding to the outbreak. Concurrently, due to the sudden global shift to teleworking, organizations have had to rapidly deploy remote systems, networks and applications. As a result, criminals are taking advantage of the increased security vulnerabilities arising from remote working to steal data, make profits or cause disruption.

This occasion has also offered an irresistible opportunity for threat actors to perpetuate cybercrime on a global scale. Social engineering campaigns using corporate logos have preyed on the fear, uncertainty and doubt of unsuspecting users.

INTERPOL's COVID-19 Cybercrime Analysis Report reveals several trends emerging as a result of the crisis, including:

– **Online scams and phishing**: Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims to provide their personal data and download malicious content. Around two-thirds of member countries that responded to the global cybercrime survey reported the significant use of COVID-19 themes for phishing and online fraud since the outbreak.

– **Disruptive malware**: A spike in ransomware attacks by multiple threat groups that had been relatively dormant for the past few months took place in the first two weeks of April 2020. Investigations show that the majority of attackers accurately estimated the maximum amount of ransom they could demand from targeted organizations.

– **Malicious domains**: With the increased demand for medical supplies and information on COVID-19, cybercriminals have significantly multiplied registrations of domain names containing such keywords as "coronavirus" or "COVID". In June 2020, 200,000 suspected malicious domains existed, affecting more than 80 countries around the world.

Europol's series of reports have revealed similar trends in European Union member states, including more targeted attacks on the healthcare sector. The agency's reports also document the criminals' ability to adapt to the crisis, as demonstrated by the surge of counterfeit and fake products on darknet marketplaces, including COVID-19 test kits, masks and pharmaceuticals. In parallel, they also point to an increase in the amount of child abuse materials available on the darknet as well as in the access of illegal websites.

Sources: INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19", 4 August 2020, https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19; Europol, "Staying safe during COVID-19: What you need to know", 6 May 2020, https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know (both accessed 28 October 2020).

1.2 The first steps to success

The primary solution to lowering the risk of cybercrime is to increase the cyber resilience of potential victims, meaning all internet-connected organizations and users. While resilience has been the main focus of the cybersecurity market, law enforcement agencies are also supporting these efforts, by raising awareness[8] and providing alerts,[9] advice and best practices.[10]

There are reasons to be optimistic on this frontier. Recent research shows an improvement in private companies' approaches to prioritizing cyber hygiene and increasing investments in cyber resilience.[11] This is also reflected in the growth of cyber insurance markets.[12] The cybersecurity market also continues to grow, boosted by huge investments in innovation, including harnessing such advanced technologies as machine learning, robotic process automation and cutting-edge encryption and mathematical methods.

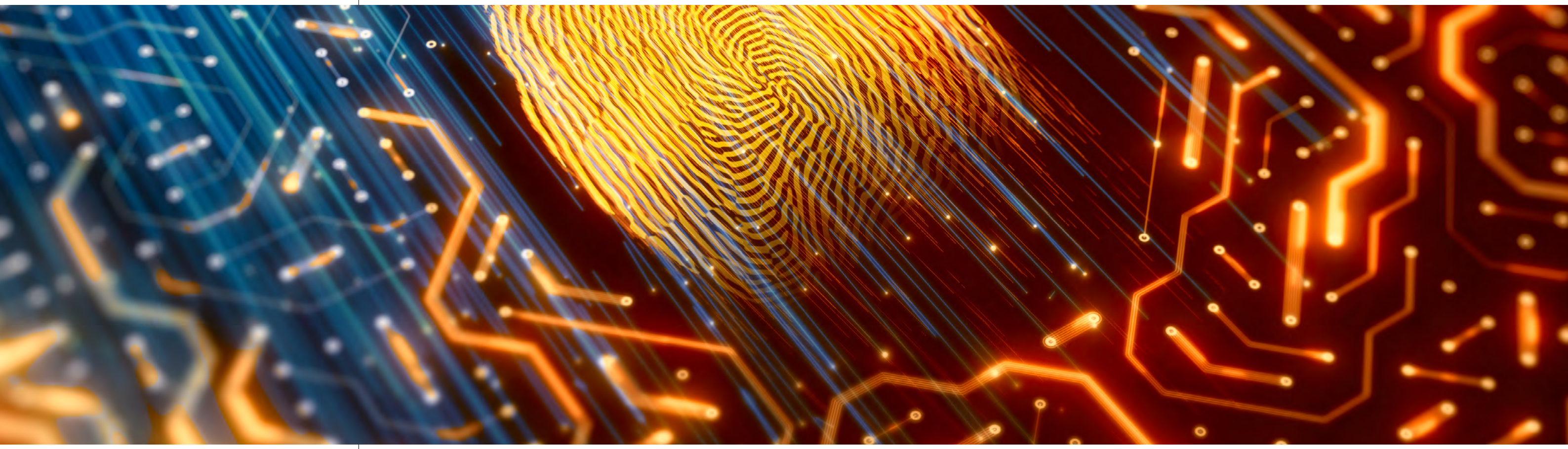
While cybersecurity efforts are mostly driven by market forces, more and more private companies are cooperating with other companies and non-governmental organizations (NGOs), significantly increasing the overall capacity to address cyberthreats. This includes initiatives usually aimed at reducing the impact of the cybercrimes on their victims. Leading examples are the **Cybercrime Support Network**,[13] which helps individuals and businesses affected by cybercrimes deal with the challenges, and **Scamadviser**,[14] which serves as a global warning list of online scams with 2 million sites added every month by more than 50 partners.

BOX 2

The victims of cybercrime

Due to the ever-increasing number of internet users worldwide, the risk and impact of cybercrime on individuals and small and medium-sized enterprises (SMEs) globally are massive. Identity theft, romance scams, ransomware and business email compromise are costing consumers and SMEs billions with few resources available for prevention, response and recovery. Cybercrime victims need a clear path to get support, just as victims of physical crimes currently have. Unfortunately, few countries have such services, notably the United Kingdom, Australia, Canada and Israel, where citizens and businesses can call one central phone number or online service to report an incident and receive advice on how to respond and recover. Governments and law enforcement agencies need to define mandates for and ownership of the response. By increasing reporting and recovery resources, countries can decrease crime and revictimization. The process needs to be clear for victims, in line with a comprehensive response plan created by governments to support them.

Several initiatives aim to make it harder for cybercriminals to operate and some reduce their potential rewards. The Europol-led **No More Ransom!**[15] project is a good example of a public-private initiative aimed at frustrating the cybercriminal business model and ultimately reducing criminal financial gain. Other efforts, such as the **Global Cyber Alliance**[16] created by the New York County District Attorney and the City of London Police Commissioner, focus on disrupting cybercriminals and the vulnerabilities they seek to exploit.



BOX 3

The global threat of ransomware

Ransomware is a fast-evolving threat. Five years ago, most ransomware attacks, with some notable exceptions, were random with a small ransom designed to entice payment. This strategy evolved into a business model in which customer service agents assist people with the purchase of ransomware services and the deposit of cryptocurrency profits, and ensure that decryption keys work, to protect their reputation. More recently, ransomware is targeted at specific organizations with large, customized demands based on perceived affordability. The malware itself is now more sophisticated, designed to act and spread quickly and even exfiltrate people's data as added leverage for extortion. The "honour" among thieves that kept targets like hospitals and critical infrastructure off the target list seems to have crumbled. The best defence for ransomware is preparation: presume you will get hit, back up your information resources, ensure continuity of operations in disruptions to the computer systems, and drill your response. Form your team in advance and include legal, technical and law enforcement members to connect you with initiatives, such as Europol's "No More Ransom!", that have a cache of free decryption tools and keys.

Nevertheless, as security and users are not perfect, cybercrime cannot be completely prevented. Cybercriminals have proven highly adept at exploiting the digital ecosystem; the risk of getting caught remains very low due to the anonymity offered by the internet and the jurisdictional challenges of nationalized legal systems, whereas the potential returns are very high. Moreover, the profits from these malicious activities allow continuous improvements in the criminals' capabilities that often surpass the cybersecurity investments made by their targets.

In the long run, in order to reduce the global impact of cybercrime and to systematically restrain cybercriminals, cybercrime must be confronted at its source by raising the cost of conducting cybercrimes, cutting the activities' profitability and deterring criminals by increasing the direct risk they face.

1.3 Law enforcement against cybercrime

Law enforcement agencies worldwide are already engaging in commendable efforts to address this threat. Countless examples of successful action exist, although the general public is not usually aware of them.[17]

Yet law enforcement agencies still face numerous challenges as they adjust to fast-evolving digital crimes. One key difficulty is limited visibility and the lack of information. Cybercrimes are likely to not be reported at all.[18,19] This situation is made worse by the anonymity and transnational nature of cybercrimes, combined with a lack of common terminology and classification of what constitutes cybercrime.

Cybercrimes are not considered violent crimes;[20] they have a significant but almost non-measurable national impact (mostly due to under-reporting). This often leads to under-prioritizing law enforcement efforts against cybercrime, the absence of clear national cybercrime strategies and a shortage of resources invested for law enforcement. The lack of resources is particularly problematic when addressing cybercrime, which requires specific tools as well as personnel with technical skills and expertise who tend to be expensive and in high demand on the labour market.[21]

Moreover, the borderless nature of cybercrime significantly challenges the structured premise of criminal enforcement based on specific geography. In the physical world, a crime occurs in a location with the criminals physically present while, in cyberspace, criminals can live in one country, carry out crimes in another, leave evidence in a third while the victim is living in a fourth. Tracking, arresting and prosecuting cybercriminals require international information sharing and cross-border operational cooperation, which are not always aligned with existing legislative and operational frameworks. These processes also require speed. Criminals operate around the clock and constantly improve their capabilities, while the sharing of information across borders through mutual legal assistance treaties tends to be painfully slow.

In response to these challenges, the international community has also started taking action to enhance national law enforcement capabilities and facilitate international cooperation on cybercrime; INTERPOL's Global Cybercrime Programme and Innovation Centre in Singapore, Europol's European Cybercrime Centre and the Joint Cybercrime Action Taskforce hosted by the latter Centre are leading results of these efforts, as are existing international policy dialogues, such as the United Nations open-ended intergovernmental expert group on cybercrime and the Council of Europe's Cybercrime Convention Committee representing the State Parties to the Budapest Convention.

However, to date, conventional governmental criminal justice efforts are proving too limited to meet the challenge. Research in the United States, for example, showed the likelihood that less than 1% of cybercrime will result in arrest.[22]

BOX 4 International and multilateral processes on cybercrime

As cybercrime rose with the introduction of digital technologies, it also steadily became part of discussions and processes in several international, multilateral and multistakeholder fora. The first multilateral negotiations that aimed to keep criminal law abreast of technological developments were launched in 1996 by the Council of Europe, resulting in the 2001 Convention on Cybercrime (known as the Budapest Convention). To date it remains the only legally binding international treaty that sets common legislative, substantive and procedural standards for cybercrime investigations and offers an international criminal justice cooperation mechanism in this field. The UN Convention against Transnational Organized Crime is another legally binding treaty with a broader, non-cybercrime-specific scope, that at times could be used to help cooperation in cybercrime cases. The international landscape also comprises several fora dedicated to cybercrime discussions, most notably the Cybercrime Convention Committee and the UN open-ended intergovernmental expert group established in 2011 to conduct a comprehensive study of the problem of cybercrime. In late 2019, notwithstanding the global scope of the Budapest Convention, the UN General Assembly decided to establish an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, which is expected to engage UN Member States in several years of negotiations. On more operational international frameworks, the Cybercrime Convention Committee's 24/7 Points of Contact Network, along with the G7 Roma-Lyon Group's High-Tech Crime Subgroup, and its 24/7 Cybercrime Network are key entities that support international cooperation in cybercrime cases and complement INTERPOL's Global Cybercrime Programme, which builds on the connections among its National Central Bureaus, its I-24/7 global police communications system, and its Cyber Analytical platform, together with its recently launched Cybercrime Knowledge and Operation Exchanges. Recognizing the dire need to support the ability of national criminal justice authorities to deal with cybercrime, capacity building has long been a consensus priority area of the international community, with prominent examples of global initiatives led by the UN Office on Drugs and Crime's Global Programme on Cybercrime, the Council of Europe Cybercrime Programme Office, and INTERPOL's Global Cybercrime Programme and Global Complex for Innovation, further to important bilateral and regional efforts.

1.4 The way forward

This threat is global – which implies that the solution must also be a globally coordinated effort. There is no single solution to reducing the harm caused by cybercrime, but it is apparent that current efforts fall short. As long as the barriers to entry for cybercrime remain low and the prosecution risk for conducting cybercrimes is limited, cybercriminals will continue to threaten societies and diminish trust in the digital economy.

It is inherently clear that a team is stronger than an individual. Individually, businesses and government organizations continue to thwart cybercrime the best way they can with some notable success. Cyber resilience and cybersecurity are a shared responsibility that involves everyone and, as such, requires an ongoing, holistic, systematic and coordinated approach. **To improve the global security posture and to increase cyber resilience, however, the public and private sectors must work together.**

2 Public-private cooperation against cybercrime

2.1 The unique role of private companies

In criminal investigations, law enforcement agencies together with the judiciary traditionally comprise the criminal justice process, with third parties outside this structure only responding to legal demands or requests for information. In this construct, the primary goal is prosecuting the perpetrators and adjudicating the crimes. However, when it comes to cybercrime, the private sector plays an instrumental role in the potential success of investigations due to a combination of factors.

First, preventing and investigating cyber incidents requires significant technical skills and capabilities. Law enforcement agencies have different levels of capabilities in some areas than the private sector, or do not have the same resources as certain private-sector organizations.

BOX 5 The role of the ICT industry

Internet service providers have unique visibility into global internet traffic, while technology and cybersecurity companies have information about the users of their products and services. This information gives the private sector insights that can be used to identify and analyse malicious activities. Moreover, in many cases, they themselves or their customers are victims and they have either direct or indirect access to systems that are being used by criminals, which creates opportunities for disruptive actions.

Second, practice has shown that companies subject to a cyberattack may be disinclined to report cybercrime incidents to law enforcement, and will turn instead to the private sector for recovery and investigation. Understandably, one of industry's main objectives in the wake of an attack is business recovery and continuity, which can be in conflict with law enforcement's objective to retrieve evidence that can support its investigation. Moreover, there is often a lack of confidence in law enforcement's ability to effectively investigate cybercrime, while at the same time there is a fear that reporting cybercrimes may also create liability or reputational risks and even have financial implications for the company and subsequent loss of public and customer trust.

Third, as a result, an organization grappling with a cyberattack is often more likely to share information regarding the incident with a contracted private-sector entity (especially security companies and professional services offering relevant services for recovery, legal compliance and attribution) or a non-law enforcement government agency, such as National Computer Security Incident Response Teams (CSIRTs).

BOX 6 The special role of National Computer Security Incident Response Teams

CSIRTs, particularly those operating at a national level, play a crucial role in protecting their constituencies by preventing and containing cyber incidents, ensuring information exchange and cross-sectorial effort coordination and, in many cases, serving as the first line of support for victims.

At the same time, CSIRTs' technical background and the data they acquire during incident management and handling processes (e.g. IP addresses, web domains) can provide valuable assistance during cybercrime investigations and for prosecution. To sustain this effort, legal and operational frameworks for cooperation need to be developed at the national level, including joint training, regular meetings and feedback loops.

Source: European Union Agency for Network and Information Security (ENISA), "Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary", November 2018, https://www.enisa.europa.eu/publications/csirts-le-cooperation/at_download/fullReport (accessed 29 October 2020).

Moreover, due to the transnational nature of cybercrimes, CSIRTs also play a role in supporting international cooperation and leveraging the strong CSIRTs international networks, founded on trust and well-aligned objectives. International organizations and fora, such as INTERPOL, the European Union Agency for Cybersecurity (ENISA) and the Forum of Incident Response and Security Teams (FIRST), are already working to enhance and expand these processes at the global level.

While swift and effective action to a cyber incident may be aimed at limiting the damage and expediting the recovery of the organization, that focus does not preclude working effectively with law enforcement agencies to increase the latter's chances of identifying and apprehending the perpetrators, which leads to a more substantial and lasting impact. Harnessing the private sector to work side by side with law enforcement officials is therefore critical to successfully combatting cybercriminals.

2.2 Bridging the gap

Private-sector efforts to address cyber risk in general, and cybercrimes in particular, are mostly focused on raising the resilience of their products, services and networks – both through preventive and reactive measures. Companies' efforts to deal with concrete attacks most often entail actions to accelerate recovery and ensure business continuity, as well as eventually to prevent future malicious activities. Using the World Economic Forum framework for global cybersecurity efforts,[23] this process could be illustrated as a continuous cycle, largely driven by market forces (Figure 1).

BOX 7

A framework for global cybersecurity efforts

Addressing the three fundamental and unchanged elements of any cyberthreat – cyberattackers, cyberattack and cyber weakness – the framework refers to three overarching, global cybersecurity strategic goals:

1. **Reducing the cyberattack surface**: Efforts aim to raise the overall difficulty of conducting cyberattacks by reducing points of weakness across systems and networks that could be exploited by malicious actors. In the context of cybercrime, this is mostly about increasing the security and resilience of potential victims.

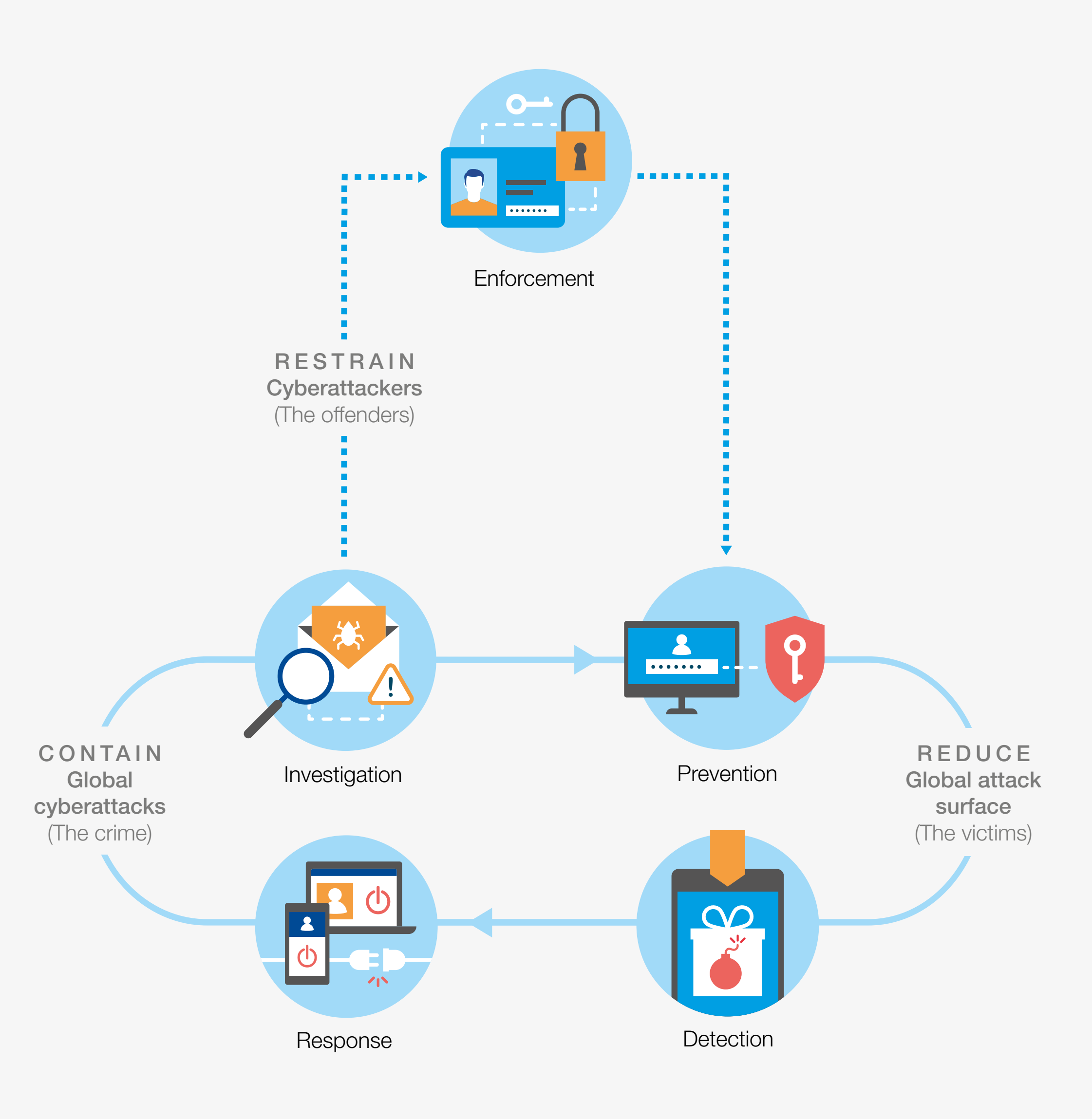
2. **Containing cyberattacks**: Efforts aim to disrupt the spread of cyberattacks and reduce their impact, usually through incident response and mitigation. In the context of cybercrime, the cyberattacks are the materialization of the crime.

3. **Restraining cyberattackers**: Efforts directly address the sources of the threat – individuals, organizations and states or, in general terms, the offenders.

Law enforcement's mission, somewhat separated from that, is to investigate the criminal act with the aim of identifying, apprehending and prosecuting the perpetrators. In some instances, however, prosecution may not be possible, but that does not mean that law enforcement has no role. It must still be engaged to investigate, identify and assist victims, and determine if the seizure of a cybercriminal's money or infrastructure is possible.

Figure 1 shows the major gap between this market-driven cycle and enforcement efforts, traditionally led by government agencies.

FIGURE 1 The gap in global cyber efforts



Source: World Economic Forum

It is necessary to bridge these two processes in a way that will leverage private-sector-led efforts and capabilities with enforcement efforts, in particular in leveraging private-sector investigations for enforcement activities and enhancing security efforts based on law enforcement insights.

2.3 Mutual benefit

While the benefits of public-private cooperation for law enforcement organizations are obvious, private organizations may hesitate to engage without understanding the positive outcomes of the process. First and foremost, sophisticated customers expect private companies, particularly technology and financial companies, to be part of the fight against crime. By participating in collaborative activities, companies can position themselves as leaders in the field and active forces for good.

As part of the collaborative process, private-sector companies will gain access to information from both law enforcement and other companies, thus increasing their understanding of the threat. This additional knowledge can allow the development of additional technical controls both internally or through products, allowing the company to protect its customers and understand the threats important to them.

Exchanging ideas and data between private-sector experts can also lead to new findings that drive product innovation, open new avenues for threat research and build communication avenues that can be used in the future to address issues outside of the collaborative framework. In short, taking advantage of collective investigation and research can potentially improve customer sentiment, drive innovation and build partnerships for future work.

2.4 The roadblocks: Challenges for public-private cooperation

The value of public-private partnerships is indisputable, yet connecting disparate organizations with different missions and goals can be difficult. Beyond the operational and cultural challenges associated with cooperation, certain policy considerations are major roadblocks to cooperation, on both sides:

– **For companies**

Conflict of information sharing with data protection and privacy laws: Two-way information sharing is a key component of any public-private cooperation. While sharing non-personal data is sufficient in many cases, operations against malicious actors require additional details, such as IP addresses, that stakeholders may be restricted from sharing due to privacy laws and regulations (such as the European General Data Protection Regulation and the US Electronic Communications Privacy Act). The challenge may increase at the international level depending on the countries where the companies are based and their obligation to comply with national privacy-related legislation that may limit their ability to cooperate internationally.

An unclear and diverse regulatory environment: In many cases, regulatory guidelines and rules are ambiguous and do not provide a supportive environment for cooperation. Companies need to take the initiative and accept certain risks associated with deciding which information, if any, and access to give to law enforcement personnel. While attempting to work against a shared threat, companies may unintentionally violate regulations, for example antitrust laws, or create liability risks for themselves. This situation hinders companies' willingness to cooperate.

Agency problems and commercial sensitivities: Voluntary cooperation with law enforcement agencies may put companies at reputational and commercial risk, if they are perceived as acting at the behest of governments or jeopardizing privacy. In some cases, commercial interests and joint operation needs may conflict.

– **For law enforcement agencies**

Restrictions on working with private companies: By law, most governments cannot treat companies with similar competencies and services differently, as dissimilar treatment could be perceived as offering a competitive advantage, for example by providing access to privileged information. Therefore, if collaboration with the private sector is not specifically mentioned in their statutes, law enforcement agencies could argue that they cannot pursue efforts to cooperate.

Evidence admissibility and availability: Companies are willing to assist law enforcement agencies by sharing intelligence relevant to an investigation, but this information is not always immediately admissible as evidence. The challenge arises when the law enforcement agency requests to receive information according to evidentiary standards (i.e. when requesting evidence from the company), which in some cases causes companies' unwillingness to share information. Moreover, regarding cross-jurisdiction requests for electronic evidence from private service providers based in another country, the current international mechanism of mutual legal assistance is time-consuming and slower than the swift action needed to avoid the loss or change of electronic evidence.

Sensitive information handling: Law enforcement information relevant to a cybercrime investigation is often highly classified and cannot be shared in a normal manner (using email, etc.), posing challenges to law enforcement agencies' ability to share information with companies. Sharing this information is necessary for meaningful collaboration on investigations but adequate security measures/controls and appropriate information-handling models must be in place to allow the sharing of information in a timely and effective manner.

2.5 Driving cooperation

Despite these challenges, many examples of successful cooperation between private companies and law enforcement agencies exist, including collaboration initiated by a law enforcement agency, a company or a group of companies. INTERPOL and Europol are both working to facilitate multinational and public-private cooperation. Leading law enforcement agencies are attempting to engage in enduring discussions with private companies. Several NGOs are working to foster multistakeholder relationships to support cooperation.

BOX 8 Existing mechanisms for cooperation

- **Cyber Defence Alliance (CDA)**: A partnership between like-minded financial institutions to jointly tackle the common threat of cybercrime by pooling resources, undertaking shared projects and sharing intelligence in a trusted environment, to improve the cyber resilience of all members

- **Cyber Threat Alliance (CTA)**: A non-profit organization that facilities both automated and person-to-person cyberthreat intelligence sharing among private-sector cybersecurity providers, and that builds partnerships with government agencies to combat cyberthreats

- **Europol**: A law enforcement agency that established the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus help protect European citizens, businesses and governments from cybercrimes. The **EC3** hosts the Joint Cybercrime Action Taskforce (J-CAT), driving EU and non-EU law enforcement agency intelligence-led coordinated action against key cybercrime threats and targets, and established advisory groups on financial services, internet security and communication providers to foster trust and facilitate results-driven cooperation with private stakeholders

- **INTERPOL**: An international organization that plays a unique role in facilitating police-to-police cooperation in the field of cyber through its Global Cybercrime Programme, providing neutral platforms for collaboration and information sharing. The **Global Cybercrime Programme** focuses on developing cybercrime threat responses and coordinating cybercrime operations and law enforcement cyber capability development; INTERPOL's Project Gateway provides one such platform for public-private information sharing on cybercrime

- **US National Cyber-Forensics and Training Alliance (NCFTA)**: A US-based non-profit organization founded in 2002 to facilitate information sharing between law enforcement agencies, industry and academia, and identify, mitigate and disrupt cybercrime threats

Frameworks and mechanisms to support, strengthen and increase cooperation in a systematic and ongoing manner need to be built. Creating new organizations or replicating existing efforts is not required; instead, overarching processes, concepts and partnerships that can complement and amplify existing efforts should be introduced.

These structures are needed not only to help overcome barriers to cooperation, but also to improve the effectiveness of the collaboration and ensure its sustainability. Also crucial is to build structures that allow the creation of truly international efforts to address the global challenge.

3 Promoting principles for public-private cooperation to combat cybercrime

3.1 The rationale

Since the publication of the World Economic Forum's Recommendations for Public-Private Partnership against Cybercrime in 2016, which outlines ways to encourage dialogues and cooperation to fight cybercrime, the Partnership against Cybercrime initiative has identified six principles for public-private cooperation against cybercrime. These principles provide a framework for action-driven cooperation that can ensure success and sustainability in collaborative activities while overcoming key challenges.

Principle 1 Embracing a shared narrative for collective action against cybercrime

The cooperation should be based on a multistakeholder approach, in which different stakeholders, while recognizing their different motivations, have joint ownership of a shared narrative and objective for the greater good of reducing cybercrime across all industries and globally.

Principle 2 Cooperating on the basis of long-term strategic alignment

Stakeholders need to commit to a long-term dialogue and to finding common ground for cooperation, based on an improved understanding of their respective needs, goals and values. The collaboration should include identifying strategic barriers to the cooperation and ways to overcome them; understanding and deconflicting respective priorities; recognizing new opportunities for cooperation and partnerships; and developing new approaches and common knowledge in support of collaborative efforts.

Principle 3 Undertaking trust-building behaviours

Successful cooperation requires a certain level of trust that allows participants to feel comfortable in the cooperation. This trust can be achieved by building and maintaining an atmosphere of transparency, equity and fairness in all interactions. Joint decision-making and voluntary sharing are important elements in building this conducive atmosphere. Interacting regularly and discussing trust-hindering actions are also needed to build trust over time.

Principle 4 Systematizing the cooperation

Cooperation should be built on institutional relationships rather than on personal relations, leveraging the respective advantages each sector brings and emphasizing common interests. This is needed both to develop sustainable cooperation that is not at risk when people change directions, and to improve cooperation when trust and personal rapport are limited. When collaborating on concrete actions, it is important to facilitate improvements by analysing successes and failures based on clearly defined objectives and expectations.

Principle 5 Ensuring value for participating in the cooperation

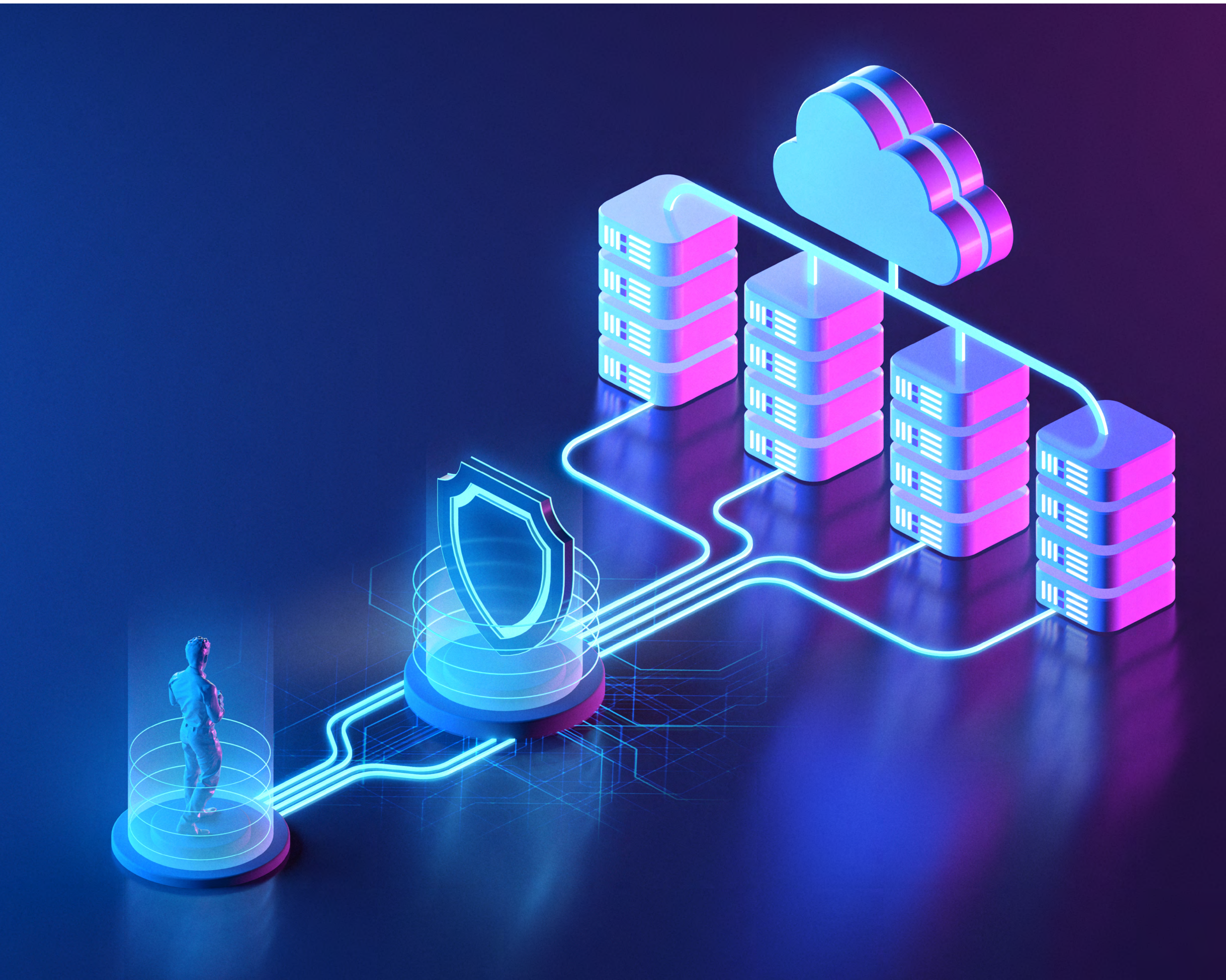
Capturing both the cooperation's concrete value as well as any other opportunities it creates is essential to ensure continued commitment and increasing investments by all stakeholders. The mutual recognition of efforts is the easiest way to achieve this when successes can be communicated publicly. Moreover, two-way feedback during and following the collaboration can also optimize value creation for both sides, while the cooperation should be supported and endorsed by their leadership to ensure that the value creation is aligned with the public and the private sectors' strategic interests.

Principle 6 Respecting concerns and challenges

All the stakeholders should acknowledge and address each other's privacy, legal and other governance and geopolitical limitations and concerns from the outset in order to pre-empt any roadblocks to the cooperation.

BOX 9 A multilevel framework

These principles are aimed at global cooperation, but they can be applied to facilitate cooperation on a regional, national or local level. Law enforcement agencies can engage with local stakeholders to improve both security and enforcement efforts. Even global corporations' national or regional operations can gain much from the cooperation at the local level. Implementing those principles normally requires some adjustment to local needs and circumstances, based on a continuous dialogue between the stakeholders.



4 Taking collaborative action to disrupt cybercrime ecosystems

4.1 Taking action against cybercrime

Traditional efforts to deter criminals have focused on raising the risks to the individual criminal actor through attribution and prosecution by law enforcement agencies and the judiciary. This approach is of course the ultimate way to stop crime. In the case of cybercrime, however, it is extremely difficult to achieve this goal by these means alone, and the chances of inefficiency and failure are high. Even the exceptional efforts of international law enforcement agencies in recent years to investigate cybercrimes and prosecute cybercriminals, and their many successes, have proven insufficient to lower the rate of cybercrime. Most often, the operations involved in investigations and prosecutions against cybercrime do not combine public-sector efforts and private-sector capabilities. The investigations have also shown that cybercrime does not resemble crime perpetrated in the physical world and thus cannot be combated using traditional methods. Instead, a paradigm shift in the way the law enforcement and private-sector communities collaborate to address this crime is required.

As mentioned, a promising way to deter cybercriminals is to raise the cost of engaging in criminal activities. One indirect way to raise these costs is to improve potential victims' cybersecurity. But, although this tactic is crucial, its results are limited because criminals often find the weakest links in the cybersecurity chain.

A more direct approach, with the potential for large-scale impact, is to disrupt cybercriminal ecosystems that contain infrastructures and assets. This approach can include taking steps to restrict revenue streams and prohibit the promotion of illegal sites and the hosting of criminal content. These restrictions can be applied, for example, by seizing the merchant account used to accept payment for the fraudulent activity or the domain that the illegal content is hosted on.

Disruption focuses on massively disabling malicious technical infrastructure. Criminals who engage in cybercrime, such as business email compromise, intellectual property theft or tech support fraud, need to lose their investments as quickly as they make them. Quickly eliminating criminal investments can inhibit their ability to execute the crime, which is especially needed when criminal activities pose an immediate danger to victims and society. In some cases, it may also allow returning some of the losses to the victims.

Private-sector companies and their stakeholders are frequently the victims of cybercriminal conduct, but they are also in a good position to lead disruption efforts. Not only do private companies have superior access to technical information and the capacity to identify, track and analyse cybercriminal activities, in many cases they have more direct or indirect opportunity to dismantle the cyber infrastructures and assets criminals use.

To date, cybercrime enforcement has been a patchwork of government and private-sector efforts to stay one step ahead of sophisticated criminals. While law enforcement agencies are used to focusing mostly on the more traditional attribution, asset seizure, arrest and prosecution approach, some private companies have taken the lead on more immediate preventive and disruptive measures, either unilaterally or through civil court action.

Effective action against cybercrime can be achieved through well-coordinated collaboration between relevant public and private actors, leveraging their expertise and advantages, exploring all possible courses of action and prioritizing joint action against the top threats. Private companies need to recognize that they have a significant role to play in not only identifying criminal trends and activities, but also in actively countering them, while law enforcement agencies need to acknowledge the unique role private companies can play and embrace cooperation as a key option. By working together against cybercriminals, they can dismantle malicious infrastructure, gather and preserve evidence for arrest and prosecution, and rescue and restitute lost assets.

BOX 10 **Disruption is here and now!**

Certain disruption operations have already proven successful. For example, in 2014, a global effort disabled the "GameOver Zeus" botnet and rescued over 1 million infected computers from criminal control. Similarly, through a public-private partnership in 2016, criminal control of the "Avalanche" network was severed and over 2 million infected computers were liberated.

These two examples show that the disruption of a cybercriminal ecosystem substantially increases the threat actors' cost of conducting their activities, and protects the public. But such actions are too infrequent and have taken too long. To effectively combat cybercrime, disruptive operations must be rapid and coordinated, applying a systematic approach and measuring their lasting impact.

4.2 Prioritizing disruption

To determine if disruption is the appropriate and optimal action, the threat should be evaluated to determine whether disabling the technical infrastructure will mitigate or eliminate the threat. But the determination is not either/or. In operations coordinated by public- and private-sector actors, a combination of traditional and disruptive approaches may work best. Working with the disruptive model along with traditional techniques will increase the costs for cybercriminals and their risk of arrest. But this combination requires the parties involved to be pragmatic, and carefully and flexibly synchronizing the action to be taken.

Managing and coordinating joint action raises certain challenges and risks. To ensure successful operational cooperation, especially when the aim is disruptive action, decision-makers should take into account three key considerations:

Operational objectives
At the operation's outset, who should participate must be considered first, including certain participants but possibly excluding others. Several factors will make a difference in the decision: for example, where the criminal actor(s) and infrastructures are located, which law enforcement agencies are already investigating, what private-sector companies (that are tracking the threat or whose services are being used by the criminal) have a stake in the case, and where the victims are located. Taking into account geopolitical factors that may influence the viability and eventual success of the operation is also important.

After participants are identified, they should determine the disruptive operation's goal. The participants in this type of operation will play different roles and may have different goals and measures of success. Timely disruptions are important to protect victims, and proper coordination can help to preserve all or most of the evidence needed for prosecution. The diverse objectives can be reconciled, but the stakeholders must identify and share their goals. They should recognize that their individual goals may not be fully achievable but should be willing to negotiate their role to support the disruption of the criminal's infrastructure.

Once it is assembled and its goals are set, the team will need to sufficiently comprehend the criminal scheme and its infrastructure to be effective.
To design an effective disruption operation, the decision-makers should be aware that the criminal investigation will not be the same as a traditional one. Traditional investigations are often narrowly restricted to attribution of responsibility and location of the underlying criminal actor. The underlying criminal infrastructure, however, is not necessarily tied solely to a single criminal actor or enterprise. Therefore, consideration should be given to the operation's appropriate scope, to achieve the biggest impact.

Legal and policy factors
To effectively disrupt criminal infrastructure, the jurisdiction(s) where the infrastructure is located should be identified. The legal authority for a public- or private-sector entity to act in that jurisdiction then needs to be clearly established. In some cases, a public- or private-sector partner will inherently possess the authority needed to act, although all actions should be performed in compliance with human rights considerations and due process safeguards. In other cases, public- or private-sector actors will need to use the authority of the courts. In cases where a criminal's infrastructure is located in a jurisdiction that does not allow coordinated action, the team may be able to identify another jurisdiction that could provide the legal authority to execute the disruption in a different way. For example, if directly confiscating the infrastructure is not possible, seizing websites could be an effective alternative when the domain registrar is located within the legal authority jurisdiction.

In addition to identifying the appropriate legal authority, it is important to consider whether the disruption could interfere with recognized rights to privacy or privacy regulations. During the operation, all information sharing should occur in accordance with applicable national privacy laws and agreements. All information should be secure, have limited access and include documented procedures for sharing. Therefore, relying upon existing sharing centres and protocols may make sharing more efficient. Transparency regarding the operation, the legal authorities involved and the results is essential, but naming all participants may not be practical or appropriate. Disruption operations should be lawful and legitimate acts designed to disable a criminal's infrastructure in order to protect the public.

Unintended consequences

Military wisdom suggests that "no battle plan survives first contact with the enemy". Therefore, any disruptive action must take into account the potential for unintended consequences. Negative consequences can result from dismantling a criminal's infrastructure, affecting those not involved in the criminal activity. For example, legitimate consumers or businesses may unknowingly – often through compromise – use part of the criminal's infrastructure. Other government entities with legitimate investigations related to national security or criminal activity could be at work. In almost all operations, unwitting victims who are using an infected device will need remediation. The team will also have to consider their legal liability, as those involved in the disruption could be held responsible for any damages. Careful consideration of possible unintended consequences to legitimate disruption activities will help to minimize the possible damage, allow for proper notice and anticipate remediation.

The disruption will likely become public and, for the identified team members, the publicity can result in retaliation by the criminals. In some instances, a disruption could be viewed as a crime or hostile act. Importantly, public- and private-sector actors must vigilantly monitor their systems to minimize any technical or financial harm and communicate appropriately with the public at large about what has happened, while allowing stakeholders to control their level of exposure.

BOX 11

"How do you defeat a botnet? (It takes a village)

"From December 2015 to October 2018, a cybercriminal ring used malware known as 'Kovter' to infect and access more than 1.7 million computers worldwide and used hidden browsers on those computers to download fake web pages. Ads were then loaded onto those pages to falsify billions of ad views, resulting in businesses paying over $29 million for ads they believed were viewed by actual human users. The botnet was part of a sophisticated infrastructure of command-and-control servers that also monitored whether individually infected computers had been detected by cybersecurity companies as involved in fraud. The botnet was controlled by three Russian nationals located abroad.

"The US Department of Justice (DoJ) and the Federal Bureau of Investigation (FBI) worked with the nonprofit National Cyber-Forensics and Training Alliance (NCFTA) to bring together multiple private-sector and nonprofit organizations to dismantle the botnet. The NCFTA played a key role by providing a collaborative information-sharing platform that enabled partners to share cyberthreat indicators, develop an operational strategy, and coordinate sequenced actions.

"Following the arrest of one of the suspects, the FBI worked with private-sector companies to reroute or 'sinkhole' traffic to prevent further victimization, executed seizure warrants to take control of 23 internet domains used by the criminals, and worked with server-hosting companies in six countries to preserve and then take down 89 servers used to operate the scheme … working closely with foreign partners – specifically, Malaysian, Bulgarian, Estonian, German, French, Dutch, British, and Swiss authorities and Europol – to assist with aspects of the investigation and with apprehending three indicted subjects for arrest and extradition.

"Within hours, a criminal cyber infrastructure that had been generating millions of fraudulent electronic bid requests per minute went completely dark. Eight defendants were indicted for their role in orchestrating the botnet and another fraudulent digital advertising scheme, and to date several have appeared and entered guilty pleas in U.S. courts."

Sources: Verbatim description taken from US Cyberspace Solarium Commission, *Cyberspace Solarium Commission* report, March 2020, p. 87, https://www.solarium.gov/report; US Department of Justice, "Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud", Press Release, United States Attorney's Office, Eastern District of New York, 27 November 2018, https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing (both accessed 31 October 2020).

4.3 Moving forward

Decision-makers should consider these three factors when assessing whether and how to participate in a disruption operation. Careful assessment of these issues and others that may arise in a particular set of circumstances will maximize the likelihood that the disruption will be successful while minimizing any unnecessary risks. Although the decision to participate in a disruption operation should not be made lightly, organizations should not be paralysed by inaction.

Applying the necessary amount of effort and taking the risks involved are justified because sufficiently large and timely disruption operations will make it more costly and difficult for criminals to rebuild their infrastructure, whether it pertain to their finances, personnel or technology. In addition, the information gained from operations will allow victim identification and remediation and can protect the public from future harm.

To fully enjoy the benefits of collaborative action against cybercrime, suitable frameworks must be put into place to enable sustainable and effective relations. Specifically, collaboration needs neutral and supportive spaces for considering these issues in a joint decision-making process.

5 Partnering to combat global cybercrime

5.1 A global architecture for public-private cooperation against cybercrime

Despite enormous investment from both the public and private sectors, current global efforts to limit the growth of cybercrime are fragmented and insufficient. The systemic containment of cybercrime will only happen when the scope, scale and speed of public-private cooperation deepens, expanding internationally and sustained over the long term. The response to cybercrime requires an equally scalable approach. This section presents an architecture for carrying out actions based on these principles, by forming a global network of stakeholders committed to the shared mission.

In facilitating cooperation, the problem is neither a lack of willingness nor a shortage of operational platforms. Law enforcement agencies, NGOs and private companies cooperate eagerly and frequently. A significant number of collaborative initiatives already exist, and multiple operational bodies dot the global cyber landscape. Instead, the problem is that these efforts remain fragmented, unconnected and sporadic. No existing architecture facilitates global, comprehensive and coordinated efforts against cybercrime, allows participants to act as equal partners, or takes into consideration both public and private equities. But building on existing frameworks and lessons learned to date in the fight against cybercrime to shape such an architecture could lead to a systematic transformation in the way the respective capacities of the public and private sectors are leveraged, and to turning the tables on cybercriminals.

5.2 Building a successful architecture

As with many efforts in the information age, a government-centric, hierarchical approach to combatting cybercrime will not succeed. Global public-private cooperation cannot be centrally managed by one organization. Regardless of other shortcomings, conflicting priorities among sovereign nations render such a structure unworkable. Instead, an effective architecture should take a different form and have the following characteristics:

A distributed structure: Like the internet itself, the architecture should be distributed, comprised of autonomous elements and connected through many different pathways. A distributed structure is the only way to achieve the scope, scale and speed needed to combat cybercrime.

Trust: Trust is essential for successful cooperation. Trust is built up over time; nothing can replace personal relationships or the confidence stemming from historical success. However, the architecture should include operational processes designed to enhance confidence and trust when personal rapport has not yet been built among stakeholders. For example, establishing business rules and using technology that provides stakeholders maximum control over their data and assets enhance their willingness to share.

BOX 12

Unlocking the potential of privacy enhancing technologies (PETs)

Privacy enhancing technologies (PETs) are a set of emerging technologies that can fundamentally reduce the risks associated with collaboration and information sharing (particularly in regulated environments). Techniques, such as federated analysis, homomorphic encryption and secure multiparty computation, are allowing to compute over encrypted data and thus enabling to process queries on each other's data without ever learning what the other party's data is.

PETs can unlock enormous possibilities of joint investigations between the public and private sectors, for example by illuminating potential data and investigative opportunities in different organizations, while keeping the organization in full control over its data.

The Cyber Defence Alliance (CDA) is currently testing the use of a PET-enabled collaborative platform with financial institutions to improve their ability to identify fraud in data by interrogating each other's systems for suspicious cybercrime activity. If successful, these trials may improve efficiency across investigation teams while maintaining appropriate privacy requirements protecting the data.

For more information, see World Economic Forum, *Cyber Information Sharing: Building Collective Security*, Insight Report, October 2020.

Flexible design: An effective architecture must cover many different use cases and deal effectively with regional variations. It must adapt to the varied public-private relationships and cultures in different communities. What works in South-East Asia, for example, will not directly apply to Europe.

Multilevel: Experience shows that small, focused groups are best at carrying out operational activities. Further, different targets require different small-group compositions. Yet, these groups require legal, technology and organizational infrastructure to succeed; large, permanent organizations are much more efficient at providing and maintaining such infrastructure. Thus, certain architectural elements need to be temporary, while others should be permanent. The temporary elements come into existence for a specific purpose, then expand or contract as needed over the course of an activity, and disband. The permanent elements provide the "infrastructure" needed when a collaboration occurs in order to avoid inefficiencies or to "reinvent the wheel".

Transparent processes: Effective cooperation requires processes that are transparent and repeatable. These processes can be technical (e.g. agreeing to a standard for exchanging information), business oriented (e.g. establishing standard procedures for conducting meetings) or operational (e.g. deciding on the methods used to engage in and coordinate actions among the members of the team).

Transparent rules: The policies and business rules governing the collaboration framework should be transparent and equitable (both in terms of the expectations and the treatment of participants). They should also incentivize team members to provide information, allocate resources and take action.

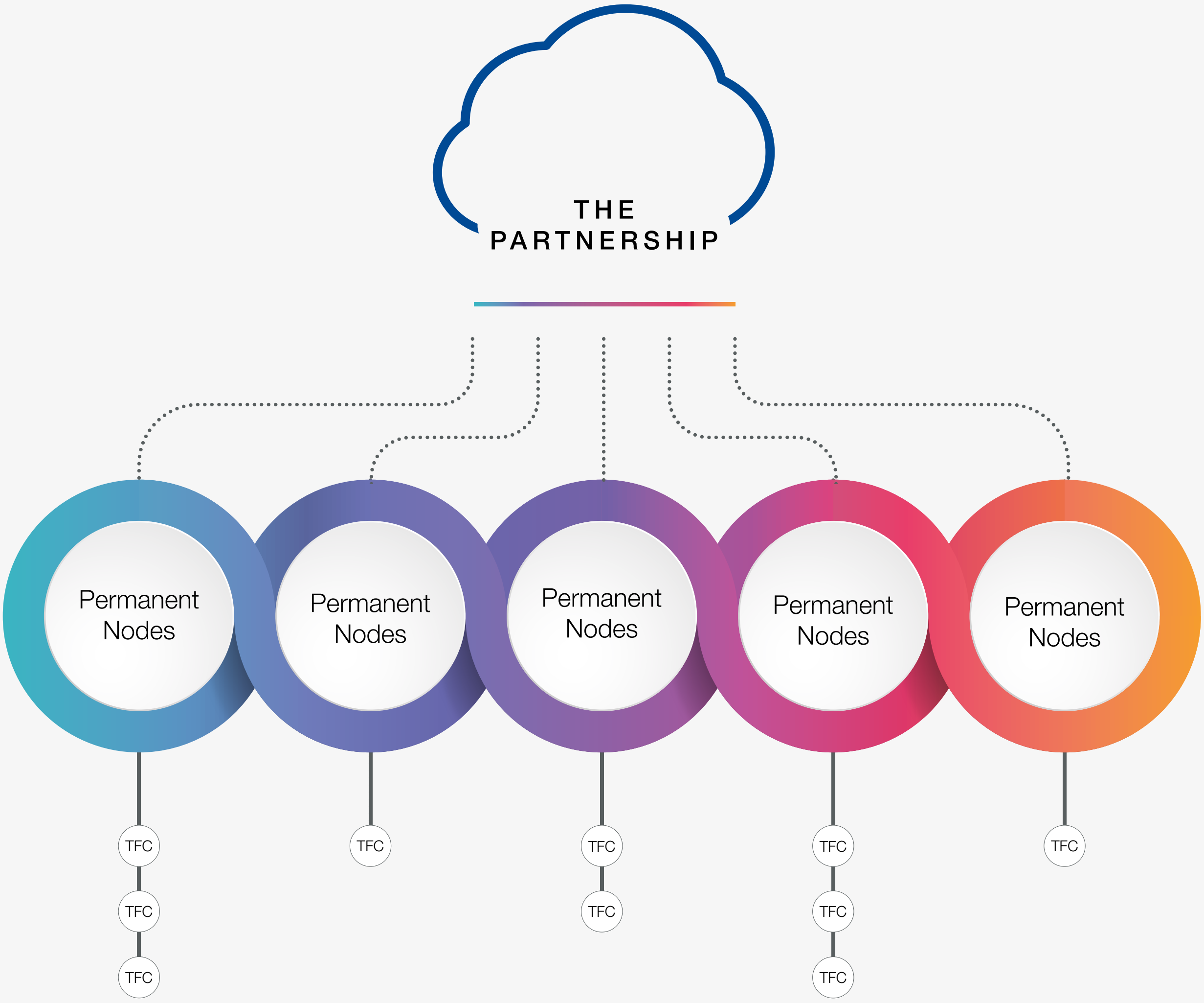
Equity: The architecture should treat the interests of all participating organizations equally and should allow the goals, priorities and outcomes of a specific cooperative activity to be set collectively; no single entity or side should dominate the process. Both public- and private-sector team members should take on leadership positions, depending on the circumstances.

5.3 A framework for success

What would an architecture against cybercrime incorporating these characteristics look like? One structure suggested by the Partnership against Cybercrime Working Group envisions a three-level system:

- **A global partnership**, building on the existing Forum initiative, to bring together international stakeholders to provide an overarching narrative and commitment to cooperate; foster interaction within a global network of entities that drive efforts to fight cybercrime; and facilitate strategic dialogues and processes aiming to support cooperation and overcome barriers in the long term.
- **Permanent Nodes**, a global network of existing organizations that strive to facilitate public-private cooperation over time.
- **Threat Focus Cells (TFC)**, short-term, mission-driven groups of partners that engage in concrete, operational, cooperative efforts. These cells will be hosted and maintained by the Permanent Nodes.

FIGURE 2 A global architecture for cooperation



5.4 A global partnership: The strategic level

A global partnership is needed to enhance commitment and harness power towards successful and rewarding collaboration, while inspiring renewed trust and confidence among the stakeholders through strategic alignment.

The partnership could be formed by building on the existing World Economic Forum Partnership against Cybercrime initiative, which brings together an action-oriented community of leading stakeholders committed to the shared goal of acting collaboratively against cybercrime.

The Partnership against Cybercrime would provide the needed strategic processes and would promote three key objectives:

– **To foster a shared narrative to increase commitment and affiliation**

  Leaders in the public and private sectors need to recognize their responsibility and ability to restrain cybercrime through collaborative action. Private companies should commit and contribute their capabilities to supporting the greater good. Similarly, public agencies should recognize the unique role private companies can play and provide space for their leadership in collaborative efforts. This narrative would also highlight the need for new approaches to combating cybercrime and the reasons traditional models, even though necessary in general, will not work in this context. Over time, embracing this shared narrative would allow stakeholders to increase their commitment and willingness to cooperate as well as build trust and affiliation between them.

– **To amplify operational cooperation**

  The partnership would facilitate insight sharing and learning between the Permanent Nodes and stakeholders, enhancing the sustainability, global reach and effectiveness of the operational processes. The Permanent Nodes would share feedback from their collaborative efforts and the partnership would support continuous learning and shared problem-solving. It would also promote improved cybercrime mapping, thereby identifying new opportunities for cooperation, and would facilitate the development of shared priorities, as the different stakeholders will have different perspectives on the global risks arising from cybercrime.

– **To improve stakeholders' understanding of respective interests, needs, goals, priorities and constraints**

  Members of the partnership would engage in an ongoing dialogue to better understand their different perspectives and to shed light on various elements that could potentially boost or hinder successful cooperation. A key effort would be to explore ways to overcome the barriers to cooperation, including working with relevant policy-makers to better address policies or laws hindering effective collaboration against cybercrime.

This global partnership's members would include the Permanent Nodes, which would host the cooperative efforts; relevant national authorities; leading cyber-related service and platform providers; large, cyber-mature private corporations; and highly targeted end users. The members would assert their willingness to participate in cooperation efforts and to support the strategic goals by endorsing the principles for public-private cooperation and the partnership's objectives.

After 2-3 years, the members of this partnership would consider transforming it into an independent entity, an Alliance to Combat Global Cybercrime.

5.5 Permanent Nodes: The coordination level

The Permanent Nodes provide connectivity between the conceptual narrative developed at the strategic level and the actions taken by the Threat Focus Cells. In particular, the Permanent Nodes provide the capabilities needed to increase and sustain the Threat Focus Cells' cooperative activities over time and to keep them aligned with the strategic goals. Neutral organizations, the Permanent Nodes would work with both public and private stakeholders equally, and would take a leading role in initiating cooperative efforts and in incentivizing participants to provide information, allocate resources and take actions.

Typical Permanent Nodes would be NGOs and non-profit organizations that are already spurring cooperation between private companies and law enforcement agencies, such as the US National Cyber-Forensics and Training Alliance (NCFTA), the Cyber Threat Alliance (CTA), the Cyber Defence Alliance (CDA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). INTERPOL and Europol, which are also leading international collaborations that include private companies, would also serve as important Permanent Nodes, allowing a much broader connection with law enforcement agencies around the world.

The Permanent Nodes' key contributions would include:

Infrastructure: The Permanent Nodes would provide the underlying infrastructure needed to make the Threat Focus Cells effective, such as communications capability, legal agreements, reporting mechanisms, office space, etc. Each activity would not require new infrastructure and multiple Threat Focus Cells could use the infrastructure at the same time.

Operational rules: The Permanent Nodes would establish, maintain and help enforce the Threat Focus Cells' technical and non-technical operational rules, such as regulating the handling of shared information. These rules would require official, legal arrangements, and should be transparent and equitable. Each Permanent Node may have a different set of rules, depending on the nature of its mission and the stakeholders involved.

Operational efficiency: The Permanent Nodes would collaborate together to reduce the Threat Focus Cells' potential overlaps or inefficiencies. They would help each other identify trusted stakeholders to fill expertise and capability gaps, and develop and implement the means to federate trust so the member of one Permanent Node may seamlessly participate in another Permanent Node's Threat Focus Cell.

Strategic dialogue: The Permanent Nodes would enable the dialogue between stakeholders to ensure a deeper understanding of the goals and priorities for concrete operational opportunities. They would also facilitate joint decisions on the goals of the Threat Focus Cells. The Permanent Nodes might also ease joint decision-making processes, taking into account operational objectives, legal and policy factors, and unintended consequences, as well as other stakeholders' concerns, such as their risk appetite, costs and reputational implications.

In this model, each Permanent Node would eventually sponsor and support many Threat Focus Cells comprised of diverse participants in varying stages of action. Choosing which Permanent Node would sponsor a particular Threat Focus Cell would depend on a variety of factors, including the Cell's level of participant representation within a Permanent Node's existing membership or the threat's disproportionate impact on a Permanent Node's home region.

5.6 Threat Focus Cells: The operational level

Under this architecture, the main operational unit would be the Threat Focus Cells. These cells would be temporary trust groups consisting of both public- and private-sector organizations and they would focus on discreet cybercrime targets or issues. Each cell would be sponsored and supported by the Permanent Node best suited for the task. The Threat Focus Cells should be able to deliver operational outcomes faster than traditional law enforcement approaches — potentially in as little as 90 to 180 days. Each cell would be in "sprint" mode, reminiscent of the agile software development approach, and it would disband upon completion. While cell structures and processes must be sufficiently flexible to accommodate the varying needs of different collaborations, consistency in a few key elements would support efficiency and interoperability:

Leadership: Ideally, each Threat Focus Cell would be led jointly by a private-sector participant, a law enforcement participant and a designated representative of the sponsoring Permanent Node. The first two co-leads should be subject matter experts and serve as the collaboration's driving force. The third co-chair would oversee the collaboration's administrative and supporting functions, such as systems access, logistics and reports, and would contribute on the substance.

Composition: Effective operations require the participation of the right organizations, or they will not achieve the desired scope and scale. At the same time, too many participants can render the activity unwieldy or erode trust. Therefore, Threat Focus Cells would typically include between 10 and 15 individual participants, based on their organizations' willingness, resources and capabilities to contribute to the collaborative efforts. Private-sector participants would typically represent organizations that can act to enhance cybersecurity on behalf of large constituencies, that have unique access to relevant cybersecurity information and threat intelligence, or that can contribute on an ecosystem-wide basis. Specialists not affiliated with these organizations but possessing needed subject matter expertise could also be invited. Law enforcement members would typically represent national-level agencies with pending investigations into the cybercrime issues being considered. Other government participants could come from network defence or sector-specific agencies, depending on the target and the nature of the contemplated operations.

Goals: All participants would need to agree on the Threat Focus Cell's desired outcomes. The goals, priorities and outcomes for a cell should not be driven by any single entity. In many cases, the goal would be a culminating operation, which could include an infrastructure takedown, public advisories and arrests. However, a Threat Focus Cell's aim could also be to scout a new threat. Identifying and arresting cybercriminals can be part of a lengthy process and are subject to considerations outside a cell's control. Thus, a long-term prosecution goal should not prevent the cell from taking other actions to protect customers and the public. However, each cell would strive to help law enforcement agencies obtain the information and technical assistance needed to prosecute those responsible for criminal activity.

Collaboration methods: Initial or periodic in-person meetings might be required to build trust, share sensitive information, establish roles, and set goals and timetables. The Threat Focus Cells would likely need to operate using remote communication. The sponsoring Permanent Node would provide the infrastructure and facilities to support this virtual work.

Operational rules: Although the Threat Focus Cells' rules would vary, a few would be common to all cells to promote efficiency and interoperability. The providing organization should clearly indicate handling requirements on shared information, for example, and the participants would agree to abide by those requirements. Additionally, participants should agree not to take unilateral action prior to the cell's culminating operation and to immediately raise any concerns to the Threat Focus Cell's leadership.

5.7 Defining success

Measuring success in cybersecurity has always been challenging. In fact, the lack of effective, widely accepted performance metrics has hindered the field's development since its inception. Nevertheless, tracking progress is necessary to correct or adjust courses of action and report on successes (or shortcomings). In addition, what constitutes success varies over time: activities that are beneficial or necessary in the short term may be insufficient in the long run. Therefore, identifying metrics on which to focus over the short, medium and long terms is recommended.

In the short term (1 year), success would be measured by the ability to convene the *community* for action and create the *conditions for cooperation*. This step will lay the foundation for taking action. To succeed in this effort, it is necessary to gather stakeholders in constructive and iterative dialogues and interactions, bridging the public-private, operational-policy and geopolitical gaps. One simple way to gauge success is by the number of stakeholders embracing the shared narrative and the principles for public-private cooperation.

In the medium term (2-3 years), success would be measured by the number of concrete and successful collaborative actions taken by the Permanent Nodes against cybercrime. This metric should reflect the specific threats tackled – in joint actions or actions supported by different stakeholders. In addition, it would be necessary to advocate for the policy processes that are needed to ensure successful and sustainable cooperation. Success does not necessarily mean a reduction of policy barriers, but the promotion of relevant solutions.

In the long term, the goal is to reduce cybercrime to an economically sustainable level. But determining whether the initiative has achieved this level of impact will not be easy. Simple percentages are impossible to calculate since the total amount of cybercrime in the world is not only unknown but is unquantifiable. As a result, gauging success will require proxy indicators. Some indicators that would point towards a decrease in overall cybercrime include a decreasing number of reported incidents; lower estimates for the economic impact of cybercrime; an increasing number and frequency of disruptive actions, including arrests and prosecution of cybercriminals; and a decreasing price for criminal services (due to decreased demand) and an increasing price for others (due to increased risk). One of the key tasks in its first few years would be to identify the most relevant, measurable and verifiable proxy indicators and determine how to track them over time.

Conclusion

Next step: implementation

The risk from cybercrime continues to grow, affecting everyone; current solutions are simply not sufficient. As long as the entry barriers to cybercrime are critically low, people will continue to suffer from its impact. Collaborative work is needed to make it harder for attacks to succeed and to make the penalties much stronger so the costs to the criminals outweigh the gains.

Businesses, governments, NGOs and international organizations must face the challenges associated with cooperating against cybercrime head-on. This report aims to help stakeholders overcome the challenges and foster the operational and conceptual processes needed. Making them a reality would be a significant step forward in this fight.

In the coming months, the Partnership against Cybercrime Working Group will continue to prepare the implementation of these concepts and widen the scope of the initiative's efforts. Leading companies and law enforcement agencies are invited to pledge their continued commitment and support to the effort to facilitate cooperation in the fight against cybercrime.

The suggested architecture could eventually evolve into a newly envisioned, independent Alliance to Combat Global Cybercrime. In the interim, the World Economic Forum and key stakeholders will work together to promote the desired processes and assess the validity of the concept.

The need to combat cybercrime is pressing and the time to act is now.

Contributors

World Economic Forum

Tal Goldstein
Head of Strategy, Centre for Cybersecurity

Nayia Barmpaliou
Head of Public Policy and Initiatives, Centre for Cybersecurity

Members of the Partnership against Cybercrime Working Group

Accenture – Jacky Fox, Howard Marshall

Amazon Web Services – Jordana Siegel

Banco Santander – Oliver Gower, Thomas William Harvey, Marina Nogales Fulwood

Bank of America – Tomas Castrejon, Dan August

BT Group – Kevin Brown, Daniel Lawrence, Alex Buckley

Carnegie Endowment for International Peace – Tim Maurer

Check Point Software Technologies – Tim Otis

Cisco – Matthew Olney

Council of Europe – Alexander Seger

Credit Suisse – Jason Mallinder

Cyber Defence Alliance – Steven Wilson, Maria Vello

Cyber Threat Alliance – Michael Daniel, Jeannette Jarvis

Cybercrime Support Network – Kristin Judge, Nichole Dennis

Deloitte – Rob Wainwright

DXC – Mark Hughes

European Commission Directorate-General for Migration and Home Affairs – Cathrin Bauer-Bulst, René J. Steiner

Europol – Philipp Amann

EY – Adam Malone, Keith Mularski

Forcepoint – Sean Berg

Fortinet – Derek Manky

Forum of Incident Response and Security Teams – Chris Gibson, Michael Bem

Ghana National Cyber Security Centre – Albert Antwi-Boasiako

Global Cyber Alliance – Mary Kavaney

Global Forum on Cyber Expertise – Christopher Painter

HCL Technologies – Syam Thommandru

INTERPOL – Craig Jones, Wookyung Jung

Israel National Cyber Directorate – Lavy Shtokhamer, Amit Ashkenazi

Microsoft – Amy Hogan-Burney

National Cyber-Forensics and Training Alliance – Matt LaVigna

Palo Alto Networks – Ryan Gillis, MK Palmore, Sean Morgan

PwC – Thierry Delville, Hugo Zylberberg

Sberbank Group/BI.ZONE – Dmitry Samartsev, Arina Pazushko

SWIFT – Brett Lancaster

Team8 – Charles Blauner

Third Way – Allison Peters

Trafigura – Mark Swift

UBS – Christian Karam, John Leo

United Kingdom National Crime Agency – Cat Wharton, Fiona Johnson, Mike Hulett

United States Department of Justice – John Lynch

United States Federal Bureau of Investigation – Steven Kelly, Mike Shanahan

United States Secret Service – Jonah Force Hill

World Bank – David Satola, Conrad C. Daly, Keong Min Yoon

Zurich Insurance – Paige Adams, Marko Hartwig

Endnotes

1. World Economic Forum, *The Global Risks Report 2020*, Insight Report, 15th Edition, 2020, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (accessed 21 October 2020).
2. Hackmageddon, "Motivations Behind Attacks (June 2019)", 12 August 2019, https://www.hackmageddon.com/2019/08/12/june-2019-cyber-attacks-statistics (accessed 21 October 2020).
3. INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19", 4 August 2020, https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (accessed 21 October 2020); INTERPOL, *COVID-19 Cybercrime Analysis Report*, August 2020.
4. Statista, "Global digital population as of October 2020", 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/#statisticContainer (accessed 4 November 2020).
5. Lewis, James Andrew, "Economic Impact of Cybercrime", Center for Strategic & International Studies (CSIS), 21 February 2018, https://www.csis.org/analysis/economic-impact-cybercrime (accessed 21 October 2020).
6. Abbosh, Omar and Kelly Bissell, "Securing the Digital Economy: Reinventing the Internet for Trust", Accenture, 2019, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf (accessed 21 October 2020).
7. Europol, "Crime areas: Fighting crime on a number of fronts", https://www.europol.europa.eu/crime-areas-and-trends/crime-areas (accessed 28 October 2020).
8. For example INTERPOL's series of cyber awareness campaigns, such as #WashYourCyberHands or #OnlineCrimeIsRealCrime.
9. For example US Federal Bureau of Investigation (FBI) alerts and complaint filing: see "Internet Crime Complaint Center IC3", October 2020, https://www.ic3.gov (accessed 29 October 2020).
10. For example US Department of Justice publications on lawful cybersecurity practices: see "Cybersecurity Unit", 12 March 2020, https://www.justice.gov/criminal-ccips/cybersecurity-unit (accessed 29 October 2020).
11. Accenture, "Lessons from leaders to master cybersecurity execution", 28 January 2020, https://www.accenture.com/us-en/insights/security/invest-cyber-resilience (accessed 29 October 2020).
12. Levite, Ariel (Eli) and Wyatt Hoffman, "A Moment of Truth for Cyber Insurance", Carnegie Endowment for International Peace, 7 February 2019, https://carnegieendowment.org/2019/02/07/moment-of-truth-for-cyber-insurance-pub-78342 (accessed 29 October 2020).
13. Cybercrime Support Network [website], https://cybercrimesupport.org (accessed 29 October 2020).
14. Scamadviser [website], https://www.scamadviser.com (accessed 29 October 2020).
15. No More Ransom! [website], https://www.nomoreransom.org (accessed 29 October 2020).
16. Global Cyber Alliance, "Enabling a Secure and Trustworthy Internet", https://www.globalcyberalliance.org (accessed 29 October 2020).
17. See Europol, "Internet Organised Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime", Europol European Cybercrime Centre (EC3), for good examples, https://www.europol.europa.eu/iocta-report (accessed 29 October 2020). EncroChat is a good use case: see Europol, "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe", Press Release, 2 July 2020, https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe (accessed 29 October 2020).
18. Only 15% of victims reported cybercrimes in 2016, according to the United States Attorney's Office, Western District of Washington. See "Financial Fraud Crime Victims", 10 February 2015, http://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud (accessed 29 October 2020). According to Donna Gregory, the head of the FBI Internet Crime Complaint Center, the number of cybercrime reports in 2016 amounted to 10-12% of all estimated cybercrimes in the United States, and a fraction of all cybercrimes worldwide. See *The New York Times*, "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported", 5 February 2018, www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html (accessed 29 October 2020).
19. UK National Crime Agency (NCA), "Cyber crime", https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (accessed 29 October 2020).
20. Concern is growing, however, regarding life-threatening cyberattacks, as shown in a recent tragic incident: see *The New York Times*, "Cyber Attack Suspected in German Woman's Death", 18 September 2020, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (accessed 29 October 2020).
21. INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19", op. cit.
22. Eoyang, Mieke, et al., "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors", Third Way, 29 October 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors (accessed 29 October 2020).
23. World Economic Forum, "Globalization 4.0: Shaping a New Global Architecture in the Age of the Fourth Industrial Revolution" (pp. 24-25), White Paper, April 2019, https://www.weforum.org/whitepapers/globalization-4-0-shaping-a-new-global-architecture-in-the-age-of-the-fourth-industrial-revolution (accessed 29 October 2020).

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org