WORLD ECONOMIC FORUM

Cyber Information Sharing:
Building Collective Security

INSIGHT REPORT

OCTOBER 2020

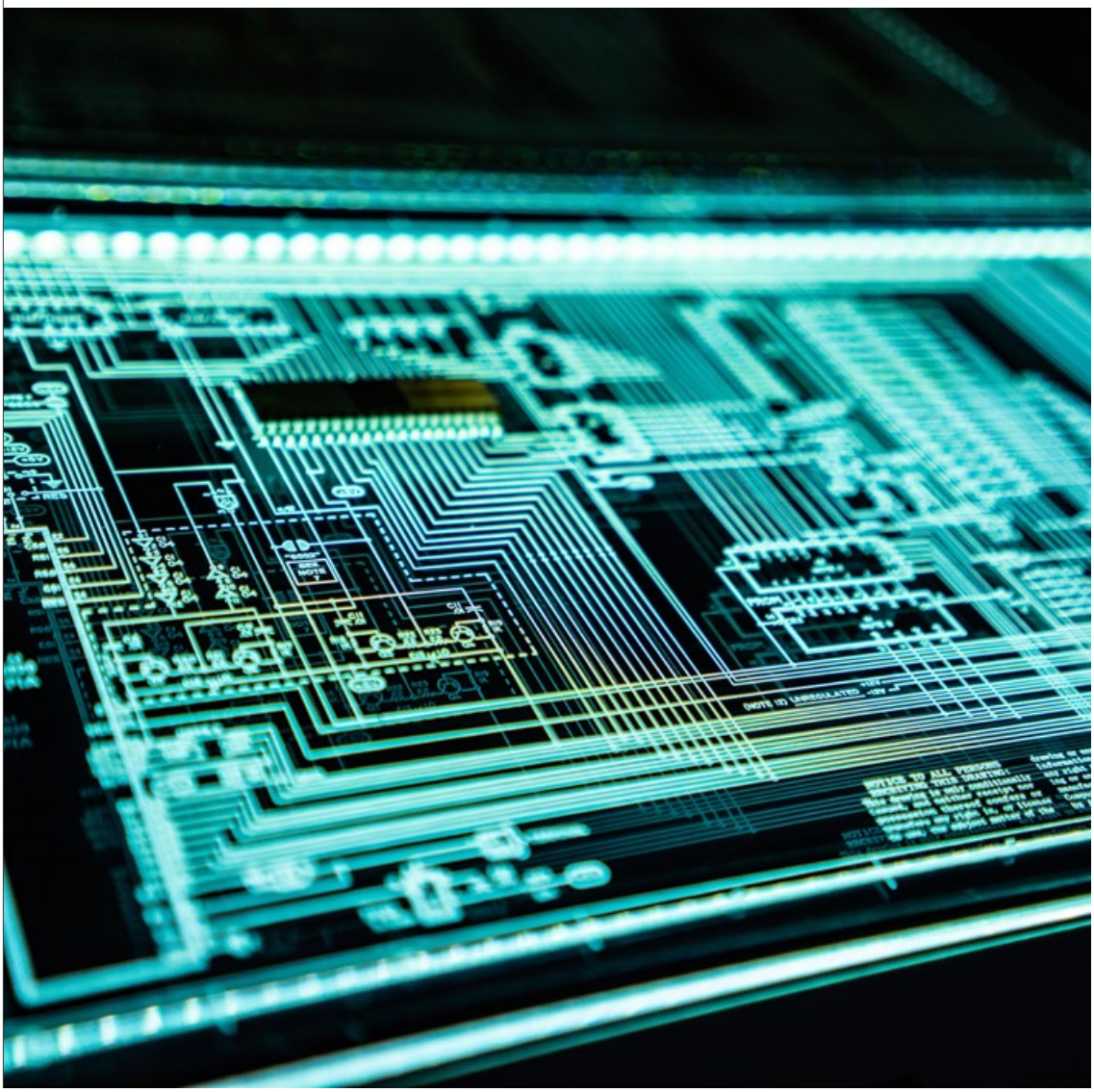
Cover: Unsplash/Markus Spiske

Inside: Unsplash/Adi Goldstein; Unsplash/Taylor Vick; Unspash/Christopher Burns; Unsplash/Uriel Sc; Unsplash/Fabio; Unsplash/Joshua Sortino; Unsplash/Zhang Kenny; Unsplas/Shahadat Rahman; Unsplash/Tetrebbien; Unsplash/Patrick Linderberg; Getty image/simpson33; ; Unsplash/Alina Grubnyak; Getty image/Orbon Alija

Contents

1 Executive Summary

Information sharing is critical for empowering the global ecosystem to move from individual to collective cyber resilience.



Intelligence sharing between stakeholders is a defining feature of the cybersecurity community and one of its most important shared challenges.

Cybersecurity is one of the most systemically important issues facing the world today. In little over a decade, cybersecurity has been transformed from a primarily technical domain centred on securing networks and technology to a major strategic topic of global importance. Cybersecurity is a pillar of a digitally resilient society. It is essential for assuring the integrity of the interconnected business and social processes that sit on top of modern societies' complex digital ecosystems. Its growing importance as an issue has been tracked by the World Economic Forum Global Risk report and now the potential impact of cyberattacks is consistently ranked as one of the biggest risks facing the global economy today.[1]

Since its relatively recent emergence the cybersecurity ecosystem has faced several challenges as it has worked to mature the isolated cybersecurity activities of actors throughout society into a cohesive ecosystem, which allows itself to be accountable to all parts of society. It has had to overcome these shared challenges in a fluid environment. The COVID-19 pandemic has led to rapid digital transformation in many workforces and sectors, further increasing the dependency of our global economy on digital infrastructure. This has exacerbated cybersecurity challenges that existed before, but also demonstrated to all stakeholders the need and incentive to address some of our most important shared challenges.

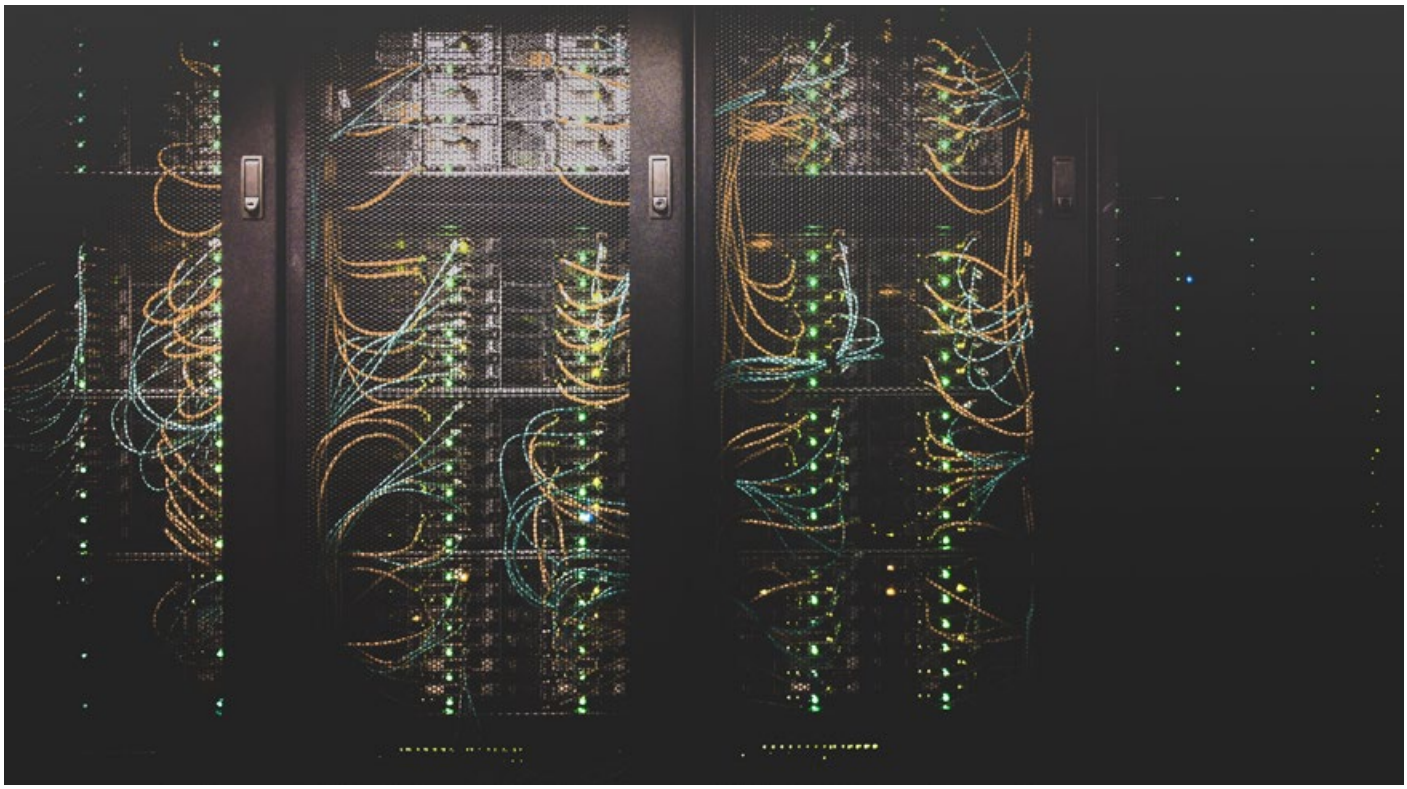
Intelligence sharing between stakeholders is a defining feature of the cybersecurity community and one of its most important shared challenges. No stakeholder alone can sustainably identify and address all the cyber threats of the fast-changing digital landscape. Trusted, secure and scalable cyber information sharing needs to be a foundational platform on which all participants of the digital ecosystem can rely.

Information sharing enables enterprises to defend themselves, enhance resilience and conduct collaborative investigations to detect and deter threat actors. It enables building trust. Barriers, however, remain in the ecosystem, including issues such as gaps in jurisdictional collaboration, in addition to cross-sector collaboration, lacking access to skills, strategy and resources, and concerns over trust and privacy. These barriers need to be addressed to promote greater resilience.

New technology, among other interventions, promises to overcome these barriers. Artificial intelligence (AI) and machine learning (ML) technologies are enhancing the effectiveness and value of sharing data, and privacy-enhancing technologies are enabling the sharing of information while protecting privacy and security. Combined, these technologies can dramatically expand, automate and improve organizations' ability to protect themselves from cyberthreats.

Ultimately information sharing is an enabler of the strategic driver of the global cybersecurity community; the need to move from *individual* resilience to *collective* resilience.

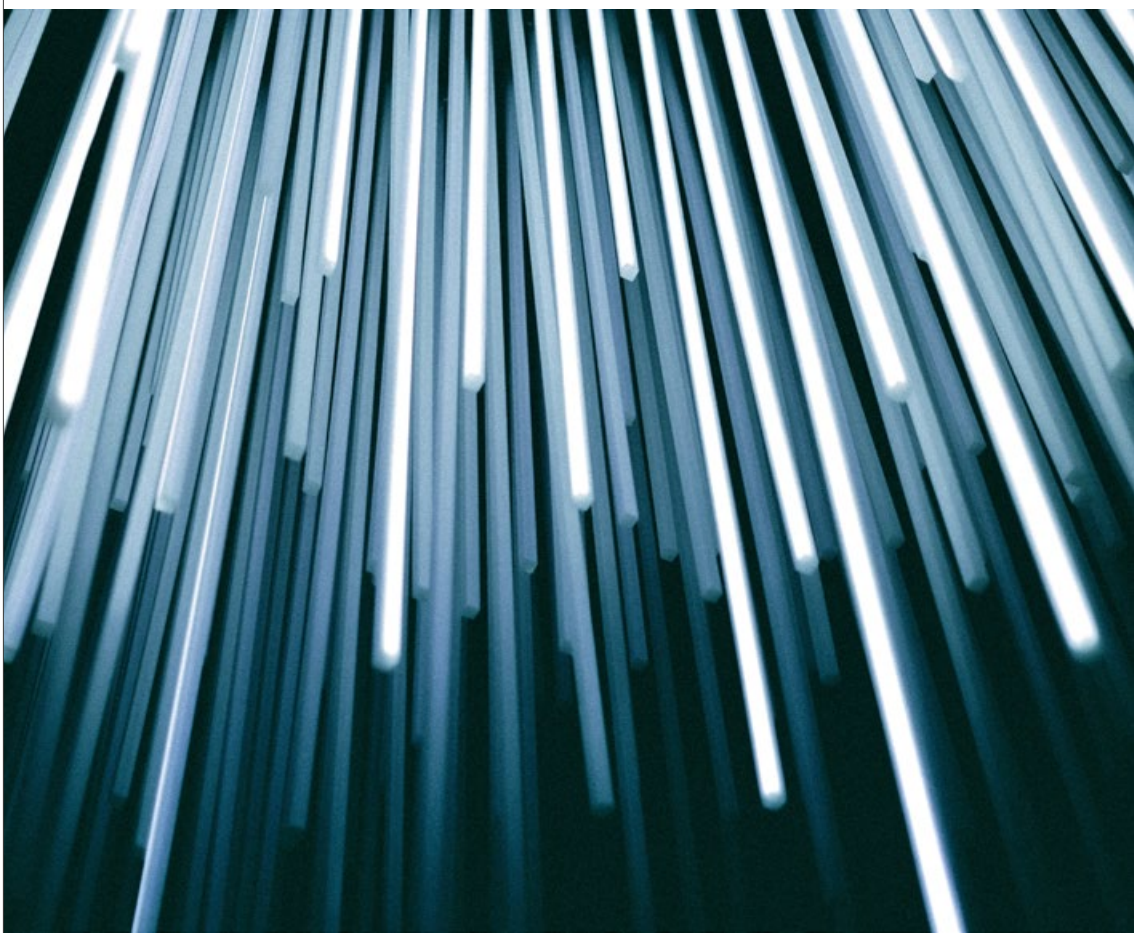
The World Economic Forum's Global Future Council on the Future of Cybersecurity, during its 2019-2020 term, focused on the nature of these barriers and challenges in the security community as well as possible new solutions. This document reflects the insights generated by this group among Council Members in addition to the Centre for Cybersecurity's extended community, including the World Economic Forum's Technology Pioneers.



2

Cyber information sharing: what is it and why does it matter?

No single organization has visibility over the entire problem space, making collaboration and information sharing essential.



Knowledge is power. Intelligence, carefully curated from the collection, evaluation and assessment of data from many sources is fundamental to understanding the complex and dynamic threats that exist in the information age. Once only the preserve of government departments and military agencies, intelligence now helps businesses and global institutions make better, data-driven decisions. It gives them the edge in formulating new plans and strategies to manage risk, and to perform efficiently and effectively.

Such is the scale and complexity of the challenge, cyberthreats and risks must be understood in detail if organizations want to prevent breaches and prosper in the age Fourth Industrial revolution. Cybersecurity is defined by its multistakeholder ecosystem and needs to be seen from a holistic viewpoint. All participants in that ecosystem need to be able to participate in building the systemic resilience of the collective infrastructure on which those stakeholders rely.

The scale of the cybersecurity challenge facing global institutions requires a mindset shift from traditional models for managing business and security risks. It is no longer feasible to rely on one's own capabilities; instead a step change will be essential to the future of business resilience. No single organization has visibility over the entire problem space, making collaboration and information sharing essential.

Information sharing and having the ability to use it helps build resilience and drives collective action. It is one of the most fundamental tools that an enterprise or organization has to protect itself. This, however, must be the right type of information sharing to solve the complex problems. Each security community is different and must define the fundamental insights required to protect itself, be this technical information or insights into strategic behaviours or trends. The ability to share the right insights at the right time in a systematic way with the right stakeholders will allow for the effective protection of assets, intellectual property and business processes.

BOX **Eight things enterprises need to be in a position to share**

There is no one-size-fits-all approach to cyber information sharing. Information-sharing arrangements between entities have to be informed by factors that take into account sector risks, as well as whether that ecosystem has sufficiently strong governance to be able to do so. Differing risks might include the nature of the cyberthreat and if the ecosystem contains sensitive or private data (such as PII, or commercially sensitive information).

1. *Observable: What activity are we seeing?*
2. *Incident: Where has this threat been seen?*
3. *Exploit target: What weaknesses does this threat exploit?*
4. *Threat actor: Who is responsible for this threat?*
5. *Indicators: What threats should I look for on my network and systems, and why?*
6. *Procedures: What does it do?*
7. *Campaign: Why does it do this?*
8. *Course of action: What can I do about it?* [2]

2.1 Cyber information sharing as a platform for collective resilience

Cyber information sharing is the ability of an ecosystem to be able to share at scale intelligence with many different stakeholders to generate the right level of *situational awareness* for organizations to defend themselves. By doing this the ecosystem can answer what has been, and what can be done about malicious activity. Organizations need to be able to do this in three key domains:

1. **Strategic:** Information that can help enterprises understand the type of threat they are defending against, the motivation and capability of the threat and the potential consequences and risks of attacks.
2. **Operational:** Information that can help enterprises' decision-making, resource allocation and task prioritization. It includes trend analysis showing the technical direction of threat actors and an understanding of malicious tactics, techniques and procedures.
3. **Technical:** Information from technical data, sources and systems that provide insights that can influence tactical decisions. This data is typically derived from near real-time monitoring and sharing of network information required for adjusting an organizations security.[3]

BOX **Information-sharing groups that are developing better cyber resilience**

- FS-ISAC: A financial industry consortium dedicated to reducing cyber risk in the global financial system. Serving financial institutions, the organization leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyberthreats.
- Cyber Threat Alliance (CTA): The CTA is a not-for-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real time, high-quality cyberthreat information sharing among companies and organizations in the cybersecurity field.
- CiviCERT: A network of Computer Emergency Response Teams (CERTs), Rapid Response Teams and independent Internet Content and Service Providers who facilitate collaboration, share information to alert emerging digital security threats to civil society and foster digital security help desks to improve protection for civil society members and organizations.

- MM-ISAC: This is a mining sector non-profit, industry owned and open to all companies in the mining and metals industry. It allows member companies to share critical cybersecurity information through secure channels, enabling them to benefit from this intelligence at a reasonable cost.

- Telecommunication Information Sharing and Analysis Centre (T-ISAC): The GSMA developed the T-ISAC to act as the sector-specific ISAC for the mobile telecommunications industry. The centre provides a place where security issues from the mobile industry can be raised, managed and discussed in a trusted environment among all GSMA members.

2.2 Cyber information sharing as a platform for collective action

Cyber information sharing can also drive *collective investigations and action* between the public and private sectors. Cybercrime cannot be addressed without creating a more effective deterrence model by confronting the source of cybercriminal activity, reducing the return on investment and making the risk of prosecution real.

Conventional criminal justice efforts are failing to limit the risks of engaging in malicious online activity. In the US, the likelihood of successfully prosecuting a cybercrime is estimated at 0.05%, far below the 46% rate of prosecution for violent crime.[4] The most successful information sharing models that are emerging in the global community and which can detect and disrupt cybercrime are between law enforcement and the private sector. Unlike traditional crime, the skills, data and capabilities to detect and disrupt cybercrime often reside within the private sector.

More are required, but these emerging models have been difficult to scale up. Sharing information between parties is fraught with potential privacy, security and due process concerns, as well as the challenge of ensuring protections for the right to free expression, association and political participation. Incentive models remain nascent, as groups try to understand who bears the cost and responsibility for driving collective action.

BOX

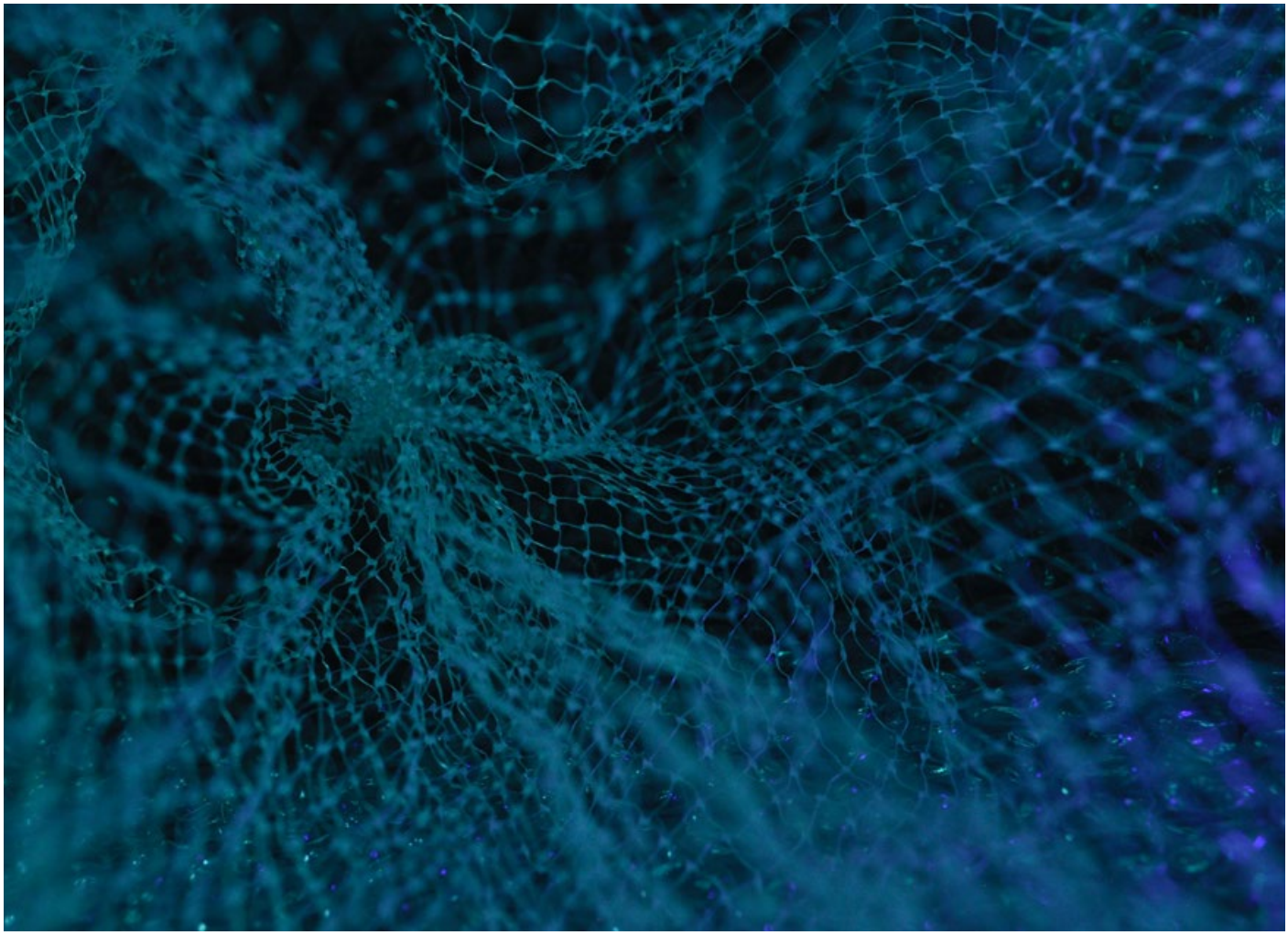
Public-private information-sharing groups developing collaborative investigations and collective action

– European Cybercrime Centre (EC3): Europol set up the EC3 in 2013 to strengthen the law enforcement response to cybercrime in close collaboration with the private sector. EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds of on-the-spot operational deployments resulting in hundreds of arrests.[5]

– The National Cyber-Forensics and Training Alliance () was established in 2002 as a non-profit partnership between private industry, government and academia, with the purpose of providing a neutral trusted environment that enables two-way collaboration. To date, the NCFTA has enabled its community to prevent more than one billion dollars in potential losses, identify critical threats and tackled more than 2,500 law enforcement cases.

– Microsoft Digital Crime Unit (DCU): The DCU is an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals based in 30 countries, working together to fight digital crime. Since 2010, the DCU has collaborated with law enforcement and other partners on 22 malware disruptions, resulting in more than 500 million devices rescued from cybercriminals.

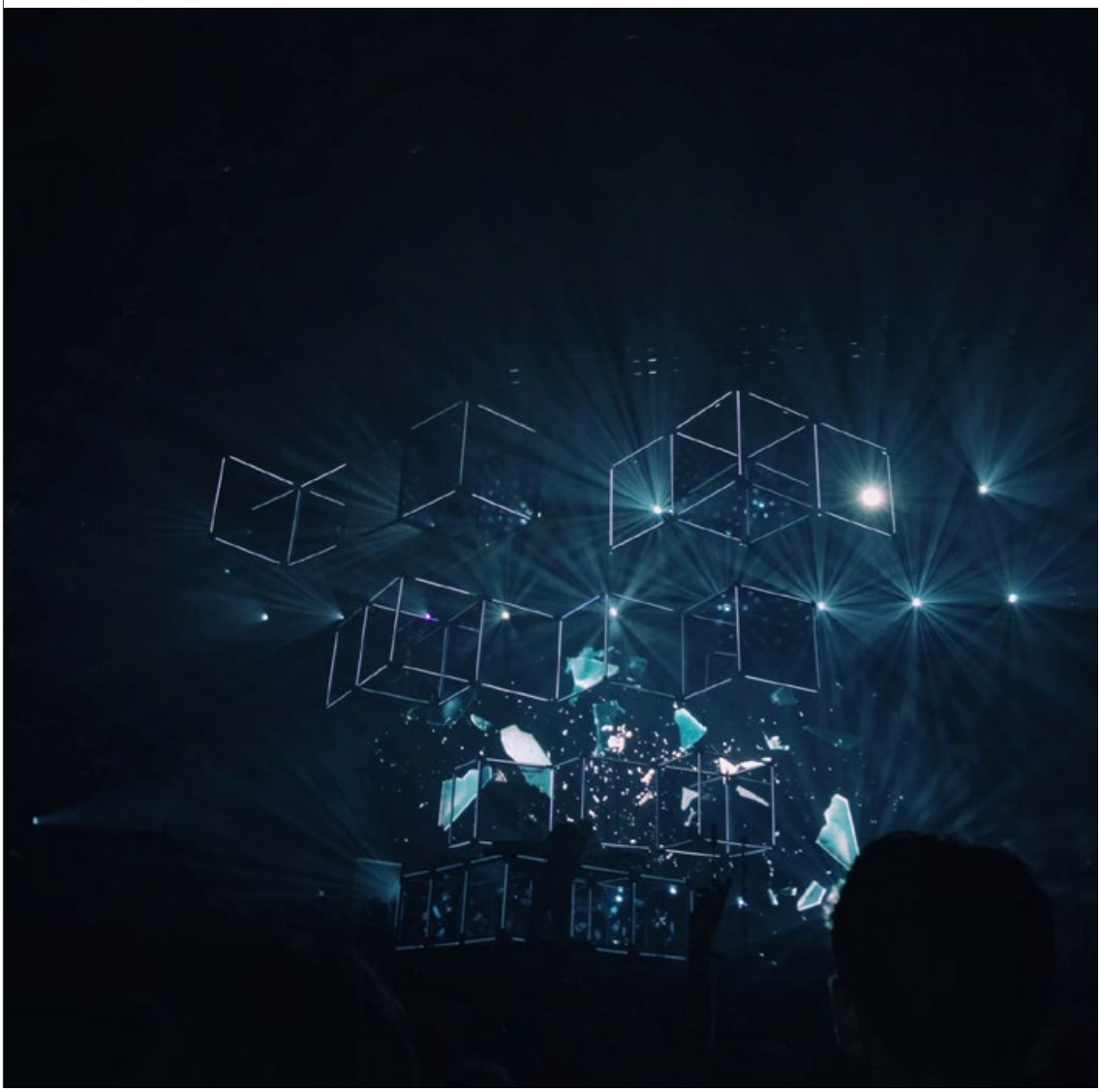
– Cyber Defence Alliance (CDA): The CDA, with its headquarters in London, is a cyber defence and anti-fraud group consortium of financial institutions originally founded by Barclays, Santander, Standard Chartered and Deutsche Bank in 2015. The CDA works with member organizations and law enforcement agencies in a co-located space to share information and turn it into actionable intelligence to prevent malicious activity and identify threat actors for criminal investigation.



3

Why does this matter now?

The Fourth Industrial Revolution demands the digitization of business and commerce. That digitization needs to be safe and secure.



There are two main drivers for why addressing the barriers to greater information sharing are of increasing importance:

1. **Digital transformation, fast development of technology and COVID-19**

   The digital technologies on which new value is dependent are what have driven the increasing importance and focus on cybersecurity as a strategic issue. A major risk to the global economy is that cybersecurity issues act as a strategic barrier to trade and that a widening digital attack surface becomes increasingly complex to defend effectively. The effects of the pandemic have made it all the more urgent to address this. Large-scale, rapid and largely unplanned digitization throughout sectors and industries has transformed the global reliance on digital infrastructure and its integrity. Cybersecurity in the wake of the pandemic was cited as the third major risk identified by global executives after the risk of a prolonged recession and the expectation of bankruptcy.[6]

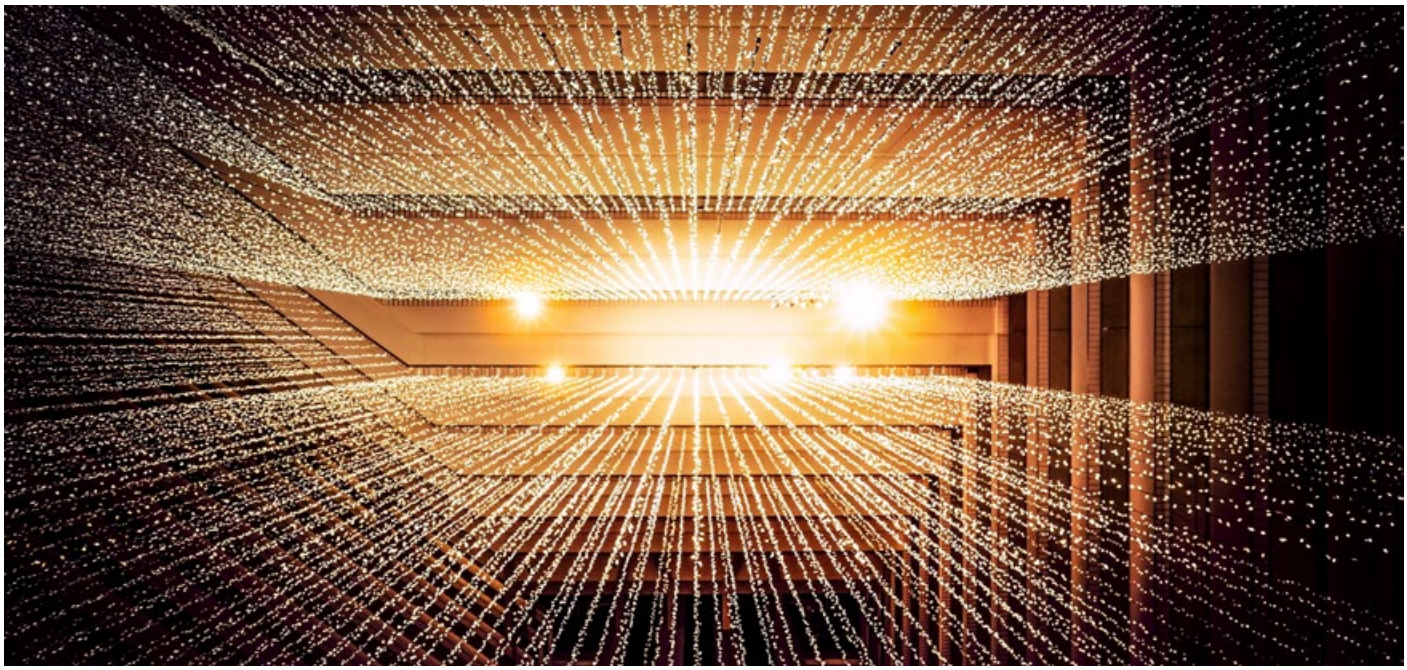
   Critically, COVID-19 has the potential to exacerbate the gulf between the cyber haves and have nots. The most well-resourced and cyber-mature institutions are now potentially at odds with those rapidly digitizing in the least mature markets and sectors, and who are also potentially impacted by major market and financial pressures.

2. **Information sharing models are not built for the Fourth Industrial Revolution and the security ecosystem**

   The digital ecosystem is not standing still. The most important technologies of the near future will alter the security landscape in a series of major shifts and not just incremental changes. New technologies will change what needs to be defended and how attackers are targeting it. This will be a major challenge to current information sharing operational and governance models as they are currently designed. If action is not taken to incentivize a new information sharing paradigm the community might not have sufficient capabilities to deliver the resilience and assurance the world is demanding.

   For example, adversarial use of AI has the potential to accelerate the scale and impact of current cyber defence approaches, but probabilistic and machine learning information sharing for network defence is still in a nascent form, and not consistently built into industry frameworks and operating models. As these AI-based information sharing and network defence systems begin to be more widely implemented they will have to overcome similar challenges to those faced by social media and technology providers in their attempts at AI-based content moderation.[7]

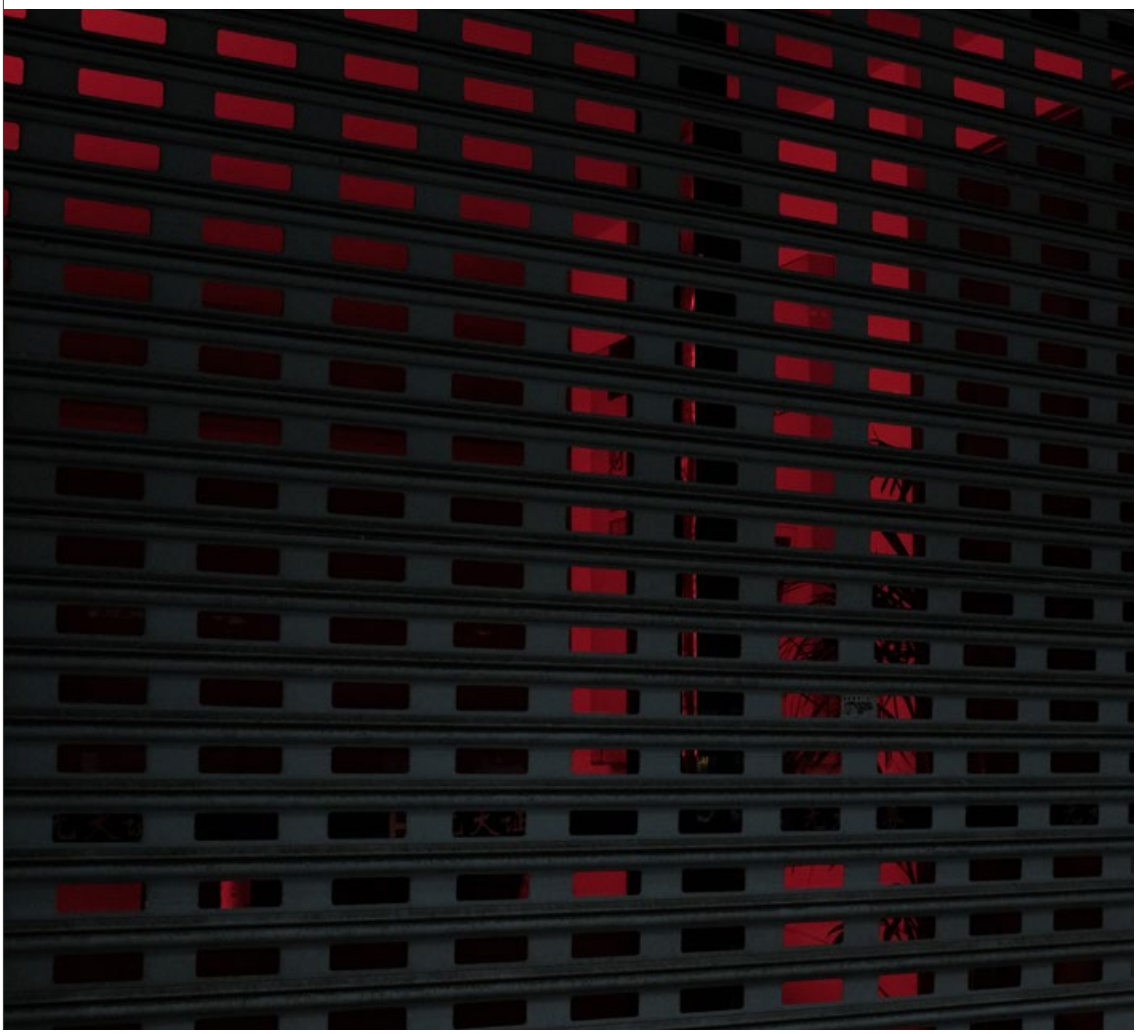
   5G has the potential to connect “Everything and Everyone” including entirely new industries, use cases and billions of devices that the security community will also need to protect.[8] Cross-jurisdictional and cross-sector information sharing will be required on a far greater scale and at a pace and complexity than the community is currently underprepared for, especially given the fact that in this new data paradigm the ability to share and act on insights will be of paramount importance.



4

Seven barriers that need to be overcome

Policy-makers, business leaders and technologists need to work together to address this global issue.



Over the past 10 years significant strides have been made in facilitating better cyber information cooperation and sharing, including the emergence of a number of different operating models (such as ISACs). This report, however, recognizes seven barriers to the progress of greater information that will support the security and resilience of the global economy.

Overcoming these barriers will require systemic improvements in cooperation, capacity and governance through the engagement of multiple stakeholders in the public, private, and civic sectors. Widespread participation in the information sharing ecosystem can be enabled by lowering the barriers to entry through widely available governance models, guidance and fundamental technology alongside clear incentives. There is also significant work needed to balance the desire to make information sharing in different sectors and across borders more effective with the need to comply with legal requirements and avoid complicity in privacy or other rights violations.

BOX **Seven key challenges the global security community needs to address**

1. **Gaps in jurisdictions and cross-sector collaboration**

   Even where there is relative maturity in sectors for information sharing, trust and barriers to collaboration remain between regions. Many information-sharing groups have emerged from, or are associated with, national legislative or regulatory authorities. Consequently, specific jurisdictions might be absent from some information-sharing groups due to wider considerations. This is the case where there are restrictions on jurisdictions collaborating.

   The greatest progress on promoting cyber-information sharing has emerged out of the most cyber-mature sectors and countries, in particular the US and European Financial Services (FS-ISAC) and in frameworks, such as provided by NIST.9 In less developed markets and sectors, however, greater progress is needed. For example, in Africa, just eight countries have a national strategy on cybersecurity and only 13 have a Government-Computer Emergency Response Team, which typically act as vehicles for establishing national information sharing programmes.10 Cross-sector collaboration as an issue was specifically part of US President Barack Obama's Executive Order 1369, which looked to establish new Information Sharing and Analysis Organizations (ISAOs) as a way of promoting more sectorial collaboration.[11]

2. **Skills and capabilities**

   The cybersecurity skills gap is well documented.[12] This pressure on resources significantly affects organizations' ability to be able to build and deploy the requisite advanced skills and capabilities to facilitate information sharing and make use of it themselves. Threat intelligence as a specialized sub-discipline of this cybersecurity skills market is particularly affected, given the skills and experience required to fulfil the role.

   In the 2020 UK Government Cybersecurity skills report, threat intelligence was listed as one of the most sought-after technical skills. Nearly one-fifth of all businesses that responded stated they had a skills gap associated with threat intelligence, which was the fourth-highest technical skill gap listed after security architecture, forensics and penetration testing.[13]

3. **Trust and privacy**

   There is a lack of trust between key players at operational and governmental levels, which needs to be developed to facilitate information sharing. Geopolitical drivers and fragmentation in international co-operation can affect public-sector enthusiasm for data exchange programmes. The private sector is often reluctant to share information with governments for fear of regulatory impact, to avoid complicity in any privacy and rights violations and because they often see no benefit to doing so. Cross-sector information sharing is further hampered by fears about giving competitors an advantage, as well as concerns about sharing sensitive internal data.

   Free cross-border information sharing is additionally complicated by the possible threats to human rights protections when information is shared with states that have a weak rule of law and or a history of systemically violating human rights.[14] The lack of sector-specific guidance tools, which map pre-existing privacy principals, responsibilities, harms and remedies to the creation and management of cross-sector information sharing has caused uncertainty. This in turn, delays efforts to build cross-sectoral programmes.[15]

4. **Legislation, policy and data fragmentation**

   There is a current lack of alignment and harmonization across jurisdictions – and in many cases *conflicting* regulations in relation to the sharing of cyber information – especially with regard to concerns over the disclosure of what could be considered as sensitive proprietary information by an organization. More dramatically the trend towards data localization – where governments mandate that data on their citizens or residents can only be stored within their country, and-or meet local privacy and security mandates before being transferred externally, can frustrate, *or outright forbid,* the fluid sharing of certain information.

The implementation of GDPR has had a major impact on the information-sharing landscape, in making some organizations fearful of breaching it. While there has been progress in jurisdictions such as the United States in providing greater legal clarity for cyber information sharing, more work is needed to provide the level of assurance required.[16] Information sharing between national and supranational authorities to drive collective investigations is also further complicated by robust disclosure and the evidential proceedings required to ensure appropriate due process and public oversight are in place.[17]

5. **Operational costs**

   To be able to effectively receive, analyse and action cyber intelligence into the full defensive posture of an institution requires investment in the right technology, staff and governance. For decision-makers and industry leaders looking to reap the rewards of participating in an information-sharing ecosystem, estimating the costs and targets for tangible investments is often difficult due to the array of options and lack of agreed standards from which to measure the benefits of such investment. Even where information-sharing programmes are available, participation costs act as a barrier. Security budgets in organizations, particularly those in developing economies, are focused only on the most immediate concerns and seldom a more holistic, mature strategy.

6. **Lack of clear incentives**

   Cybersecurity information sharing lacks traditional, positive incentives (the tangible short-term protective benefits, liability protections, insurance incentives) and negative incentives (compliance requirements, regulatory pressures). Organizations are often concerned about reputational damage or legal exposure for revealing the particular attacks they experienced, especially if the attacks were neither avoided nor defended as well as the firm would have wished. Additionally, other incentives such as cyber insurance don't currently specifically state whether organizations have an active cyber information-sharing programme. Without tangible short-term incentives in place organizations are not likely to prioritize cybersecurity information sharing.

7. **Operational, interoperability and technology barriers**

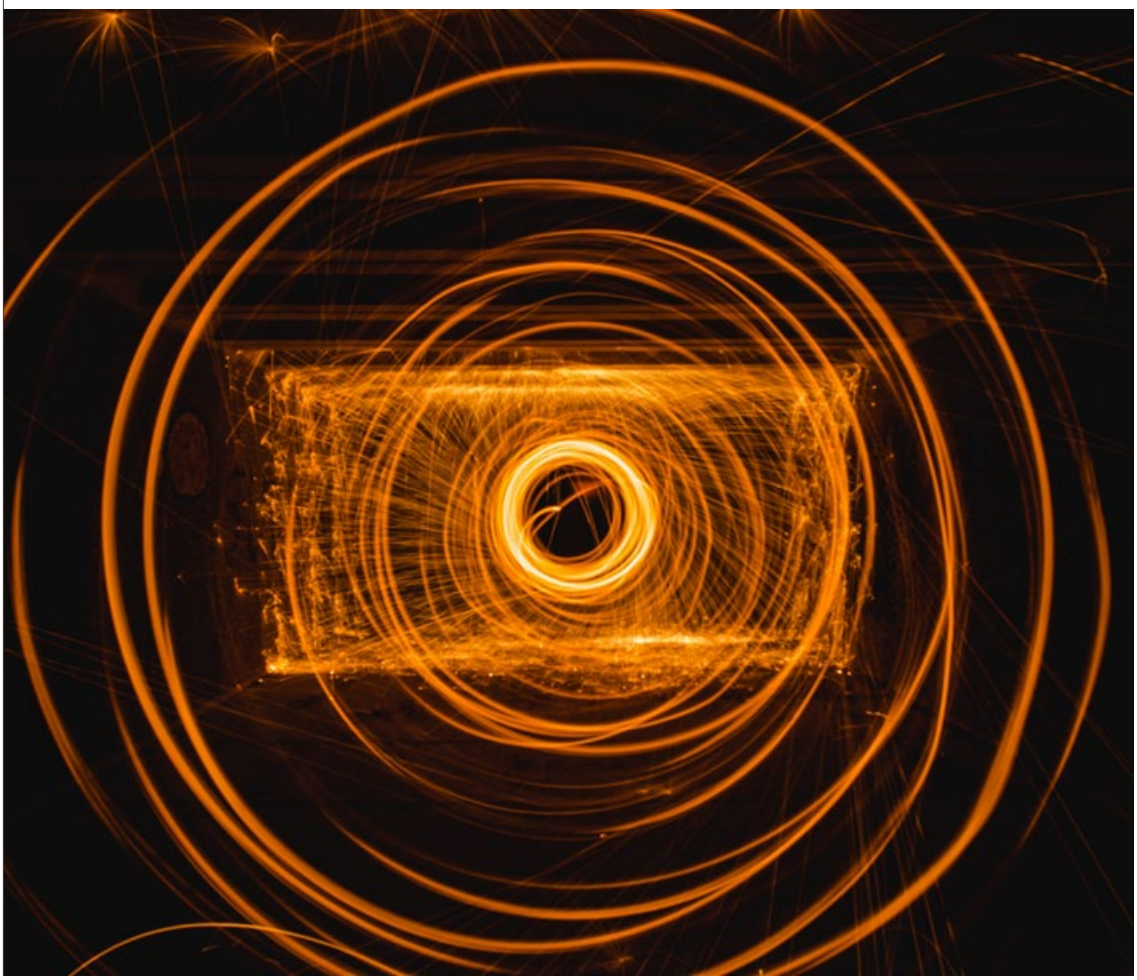
   Multiple standards, frameworks and technologies exist in relation to cyber information sharing presenting a further barrier to widescale adoption. Technical standards authorities, national bodies and certain sector groups implement specific solutions attuned to their environment, but more work is needed to be able to provide interoperability throughout the ecosystem to ensure cyber information-sharing practices can be harmonized. The lack of harmonization not only makes interoperability difficult, but it forces privacy and other rights-based considerations to be re-evaluated for each new standard and/or framework creating additional unnecessary hurdles.

   While there are no-cost and open-source technologies such as MISP, The Hive, Cortex and IntelMQ, there are still significant technical resources required to implement technology to create and/or participate in cybersecurity information-sharing communities. This can reduce the overheads of producing information and/or refining others' information into actionable intelligence, or allow easy integration between threat information sharing feeds and the range of security/investigation tools used by defenders.[18]

5

Information sharing 2.0: how next-generation technology can help

AI, ML and Privacy Enhancing Technology can enable a new information-sharing paradigm.



To address the barriers that exist more work is needed by the community to enable a new information-sharing paradigm. If we are to succeed in secure our digital networks, this new paradigm will require bold leadership, new policy frameworks and the application and use of transformative technologies. These technologies will accelerate our collective ability to overcome many of these current barriers and better ensure our collective resilience.

Fundamentally, there are two types of new technology that can aid the community in overcoming these barriers.

1. **AI and ML** technologies that enhance the **effectiveness and value** of shared data.

2. **Privacy enhancing technologies** (PETs) that enable sharing while protecting **privacy and security**.

Both categories are independently useful. The high potential is the combination of both to build a resilient digital ecosystem. Effective sharing is only possible if privacy and security are ensured, and incentives are obvious.

5.1 AI and ML

AI and ML are potentially transformative for cybersecurity and the information-sharing landscape. It dramatically expands the amount of data available to security teams and researchers at the same time as automating and scaling up the analytical and defence capabilities of organizations.

An important first step towards facilitating the information-sharing process and being able to operationalize the data is having standardized formats and shared, interoperable platforms. These are, however, primarily designed to facilitate the sharing of highly technical data such as indicators of compromise (IoCs), which are generally low-level, structured data. This definition needs to be expanded to include everything from unstructured *raw data* (e.g. network flows) to unstructured *insights* (e.g. Tactics, Techniques and Procedures (TTPs)).

Many attacks are diagnosed through the manual analysis of highly technical data, which is fundamentally not scalable. More importantly, these analytical skills are highly sought after, expensive and generally not available to the vast majority of enterprises. Consequently, there is an urgent need to incentivize tools to *automatically* extract meaningful cybersecurity insights from such data without human intervention.

AI and ML have been immensely successful in extracting insights from big data in other domains. Historically obstacles to the deployment of AI/ML are rapidly being overcome by the cybersecurity community and their technical efforts are centred on three key pillars of capability:

1. **Clean data –** Data is now produced in more shared standards than ever before. Enterprises that have enough relevant attack data can now train reliable defensive models, especially if that data is labelled, indexed and of high quality. AI can help by cleaning up previously unstructured data using the latest techniques in Natural Language Processing (NLP). This will make vast amounts of previously unusable data available for sharing and analysis.

2. **Reliable algorithms –** With clean data, comes the ability to generate reliable algorithms. Deep learning in particular has led to the development of algorithms with remarkable accuracy levels. These means enterprises have higher detection rates with less false positives, which makes them more likely to be able to put into production and enhance organizations' defensive postures. These advances have made AI systems accurate enough for many corporate defensive systems (where risks around false positives may not lead to liability). But far greater precision may be required for AI systems that collect and share information as false positives in those systems that could lead to inappropriate sharing of personal and or proprietary information.

3. **Explainable AI –** With clean data and reliable algorithms, enterprises can start to put appropriate governance and standard operating procedures in place. The security community has been able to make strides in the field of *interpretable AI*, which aims to design models that produce outputs *and* explanations for outputs. Defenders are now able to understand and explain the rationale of any automated decision-making in the models and systems, including for full accountability and audit. Addressing many current and future legislative challenges related to information sharing will require that all decisions made by AI-based systems will need to be explainable. AI systems used in information collection, sharing and use that cannot provide satisfactory answers to legal questions posed against them will likely become barriers to information sharing.

5.2 Privacy Enhancing Technologies

PETs are another set of emerging technologies that have the potential to alter the cybersecurity and information-sharing landscape. PETs can give assurances to senior leaders that the benefits of data sharing can be realized at the same time as adhering to data protection and privacy requirements as well as managing corporate risk by "enabling the analysis and the sharing of insights without requiring the sharing of the underlying data itself". [19] These technologies will be essential for the future of information sharing because overcoming lacking trust or legal mandates will demand that systems have safeguards in place to protect against malicious attempts to access and/or derive sensitive data from within them.

Specifically, this could be transformative for enabling joint investigations between the public and private sectors, which can drive collective action. These technologies could be used to identify potential data and investigative opportunities in different organizations and jurisdictions with high levels of assurance and integrity without sharing the data with each other directly. For private companies, the ability to secure shared data across jurisdictions or silos within their own organization as well as with work collaboratively using sensitive data with third-parties opens the door to a number of business use cases that are currently restricted or prevented by regulatory and legal barriers.

As outlined in the World Economic Forum's whitepaper on PETs – there are two important categories of techniques that can underpin next generation information-sharing programmes.[20]

1. **Encrypted computation:** a suite of algorithms that enable parties (particularly in low-trust environments) to compute queries on each other's data without ever learning the other party's data, including federated analysis, homomorphic encryption, zero-knowledge proofs and secure, multiparty computation.

2. **Differential privacy:** can be used to limit the amount of private information leaked by the results of these queries, shared data or models by adding noise to a data set so that it is impossible to reverse engineer the individual outputs.

5.3 Encrypted computation

The ability to make analytic computations over data that is *already* encrypted could represent a transformative shift for organizations looking to collaborate with a wider ecosystem of partners while maintaining complete confidentiality, security and managing associated risks.

Data has three basic states: at-rest, in-transit and in-use. Organizations that handle sensitive or confidential data typically protect the privacy and confidentiality of their data by encryption.

Traditionally, encryption is used to protect data when it is at-rest or when the data is in-transit. Whenever data needs, however, to be processed, analysed, manipulated or used in any way, the data needs to be decrypted – leaving the data vulnerable, particularly when shared and analysed by third parties.

Algorithms such as Homomorphic Encryption (HE) can start to address this strategic issue. HE allows computations to be performed on encrypted data, thereby keeping data secure throughout the data lifecycle. While the mathematical theory has been known for some time, recent advances have accelerated the potential real-world applications and made HE practical for computations on data sets, and its ability to perform at scale. The technology is now rapidly moving to global standards and there are open consortiums that are working together to ensure global interoperability and accessibility of the technology.[21]

HE alleviates the need for a trusted third party by also enabling the encryption of analytics as well. Protecting the privacy of sensitive data, analytics and AI models, this opens up new ways in which multiple parties can collaborate to glean deeper insights while overcoming trust and security challenges.

Organizations that are pioneering this technology for information sharing are now seeing these benefits:

- **Secure and federated data analysis**: organizations can have their encrypted data analysed by AI and analysts without revealing the underlying data

- **Secure data linkage**: multiple organizations can contribute encrypted data for joint analysis and investigations

- **Secure search**: organizations can send encrypted queries to one-another's databases without revealing the details of their query

- **Privacy-preserving machine learning:** can encrypt AI models, protecting the model itself while preserving accuracy

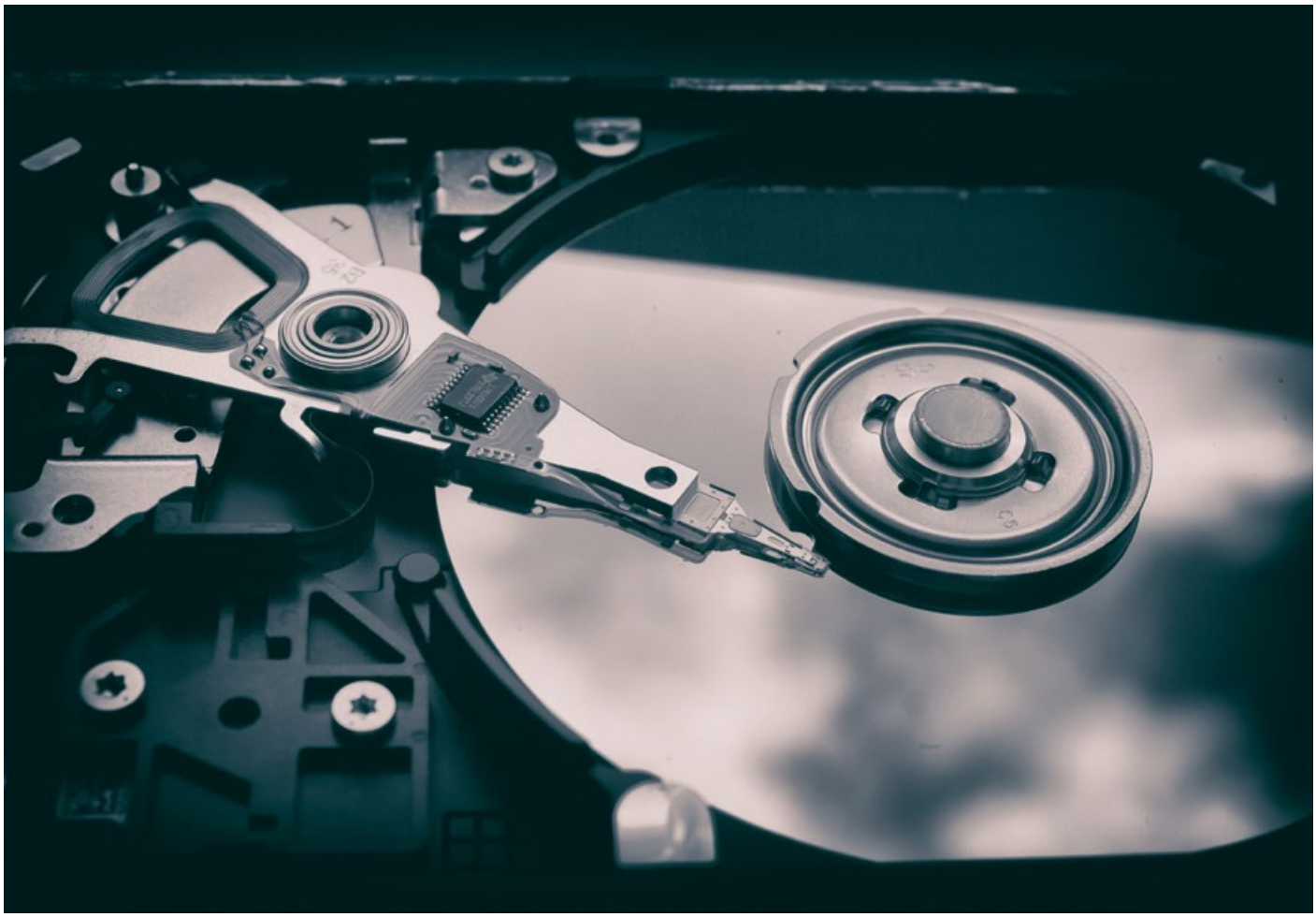
In the future, investigative authorities and the private sector could be further enabled by advances in Secure Multi-Party Computation (SMPC). SMPC uses a set of cryptographic protocols that distribute a computation to multiple parties, so no individual party can see the other parties' data and nobody sees the complete set of inputs, thereby rendering any intercepted data between parties worthless.

5.4 Differential privacy

For some parties who are sharing cyberthreat information, a further level of protection may be required. While the previous approaches protect organizations' data through encryption, the *results* of encrypted data analytics can, in some cases, reveal sensitive information. For example, AI and ML models can leak information about the data that was used to train them, *even if the model was trained entirely on encrypted data*. Fortunately, there exist techniques for ensuring that the final outputs of data analytics pipelines do not leak sensitive information about the underlying data (e.g. PII).

Differential privacy is one leading such technique, which is used today by companies like Google and Apple to collect data from their users without compromising the users' privacy. Roughly, it works by *altering* learned models to ensure that no single piece of input data contributes too much to the final model. Differential privacy is part of a broader class of privacy techniques that rely on obfuscation rather than encryption. It is performed by altering the *statistical* properties of data or models to prevent adversaries from reconstructing the original data. Classical data techniques for obfuscating PII (e.g. redacting data, releasing only aggregated data) are examples of obfuscation techniques with weaker privacy guarantees than differential privacy.

Differential privacy is an active field of research and several challenges remain regarding its practical implementation and applicability. Chief among them is that differentially private models tend to have worse accuracy than non-differentially private ones. In general, the stronger a model's differential privacy guarantee, the worse the model's quality. For enterprises charged with defending their networks in real time, more work needs to be done to understand the practical applicability of such models that balance privacy and sharing actionable insight.



6

CDA case study: using PET to drive collective action in the cybercrime ecosystem

It takes a network to defeat a network.

The Cyber Defence Alliance (CDA) is a non-profit public-private partnership headquartered in the United Kingdom that worlds collectively and collaboratively throughout the financial sector and law enforcement to proactively share information to fight cybercrime and counter cyberthreats.

The CDA was established as a way of building trust between its founding members and law enforcement authorities to be able to proactively detect and disrupt cyberthreats. Its core capabilities are centred on members being able to share information and this be enriched and analysed to provide actionable intelligence for industry and law enforcement.

The cybercrime economy operates as a platform business, with groups of specialists taking specific roles or providing services to complete the end-to-end business processes needed to successfully commit crime.[22] There are two broad, interconnected sets of criminal services:

- Technical services that provide the infrastructure and expertise for attacks, exploitation vulnerabilities and gain access to sensitive data and networks to then be monetized

- Cash-out and laundering services to enable the successful monetization of stolen data

To identify and disrupt these types of criminal services, law enforcement must collect data from a wider range of sources than ever before. Major barriers exist, however, in being able to quickly and proactively identify relevant sources and follow strict procedures to compel institutions to provide any pertinent data linked with potentially malicious activity. Consequently, acting at pace to be able to detect and investigate potential cybercrime-linked activity is often delayed by the inability to coordinate multiple parties, data sets with the correct request, authorities and disclosure processes. Criminals exploit these gaps to evade detection.

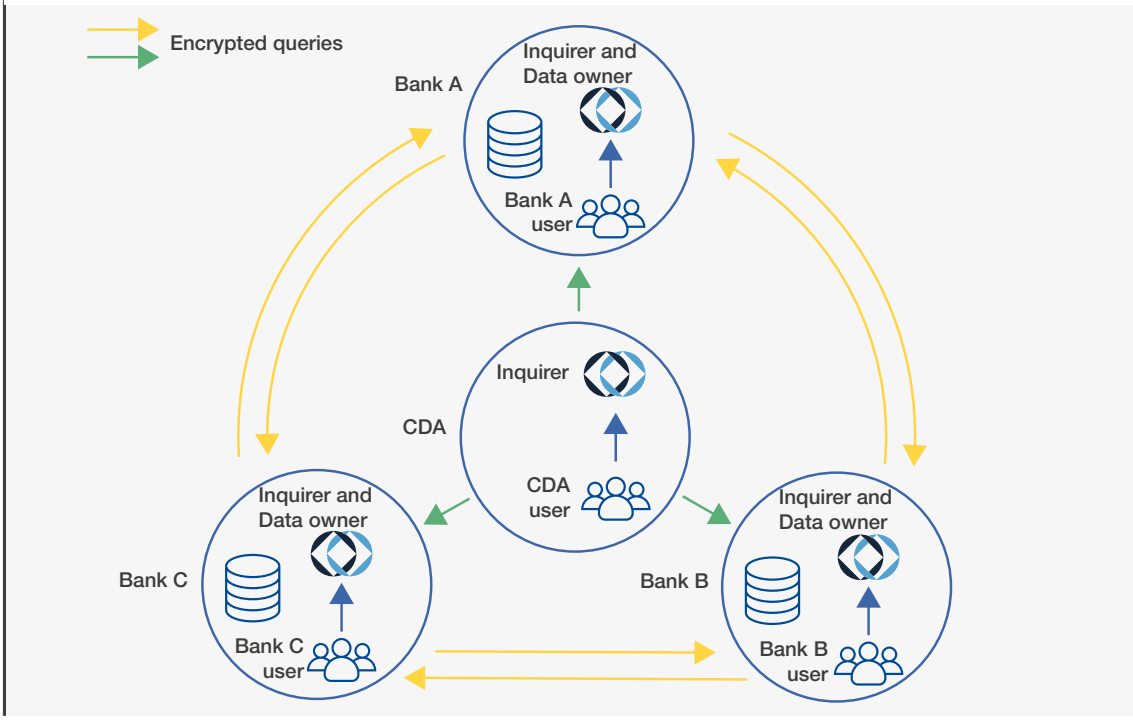
Federated data analysis powered by the ability to compute queries over encrypted data offers a step change to this process. PETs and legal provisions protect the disclosure of information, but the data is accessible for analysis and matching between institutions enabling them to conduct collaborative investigations.

The advantage of a privacy preserving analytical capability, is that it can enable the distribution of tactical search queries, without disclosing the search terms to the authorities. This negates the risks of disclosure and regulatory breach, while providing an investigative capability for authorities throughout multiple entities.

6.1 The pilot: secure and confidential querying

Within the CDA, a consortium of four global financial institutions and the UK's Metropolitan Police used a PET-enabled collaborative platform to improve their ability to identify fraud in data by interrogating each other's systems for suspicious cybercrime activity. Intelligence requirements and data sources were pre-agreed by all participants. This allowed the automatic exchange of data across participants' systems, saving time resources for investigative teams while retaining a higher level of integrity than previously.

FIGURE **PET and joint investigations**



Source: duality technologies.

6.2 Results

The CDA is a pioneering case study for a potential future operating model of cybercrime investigations. By coordinating an interoperable solution throughout multiple commercial parties and public authorities sensitive search parameters pertinent to cybercrime investigations, including PII, account numbers, transaction data and competitive information, remained encrypted during the process so that the subjects of investigations remained protected at all times.

Compliance and preservation of privacy and confidentiality: Encryption protects the sensitive query details. No sensitive data was exposed during the process. Confidential querying also prevented insider tip offs, which could have seen suspicious accounts closed before law enforcement had been able to continue the investigation with the bank in question.

Timely responses from partner banks enabled more efficient responses to detect and deter malicious activity. For law enforcement this ability meant being able to take proactive, timely action that ensured they could stop funds before they were transferred further through the laundering network.

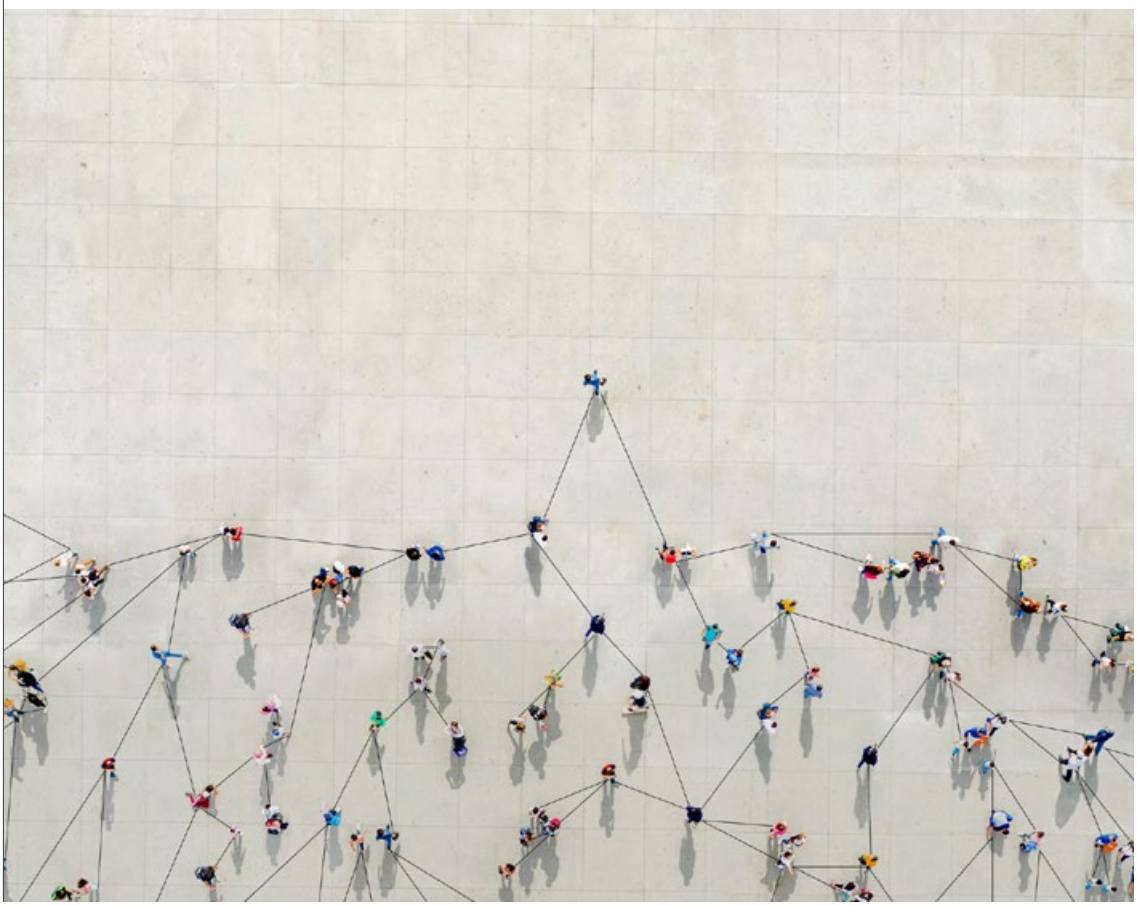
Improved attribution and case building by banks and law enforcement (as a result of better information delivered in a timely manner), reduced criminals' return on investment and potentially their ability to operate.

> **Until now it's been like Sophie's choice — guaranteed privacy of sensitive data versus supporting the fight against criminality. HE means we keep both — sharing insights without sharing customer details**
>
> Paul Branley, Director of Strategy and Innovation, Lloyds Banking Group

7

CONCORDIA: an ecosystem for collaboration

A platform joining up information from disparate data sources and sectors; a single view for security.

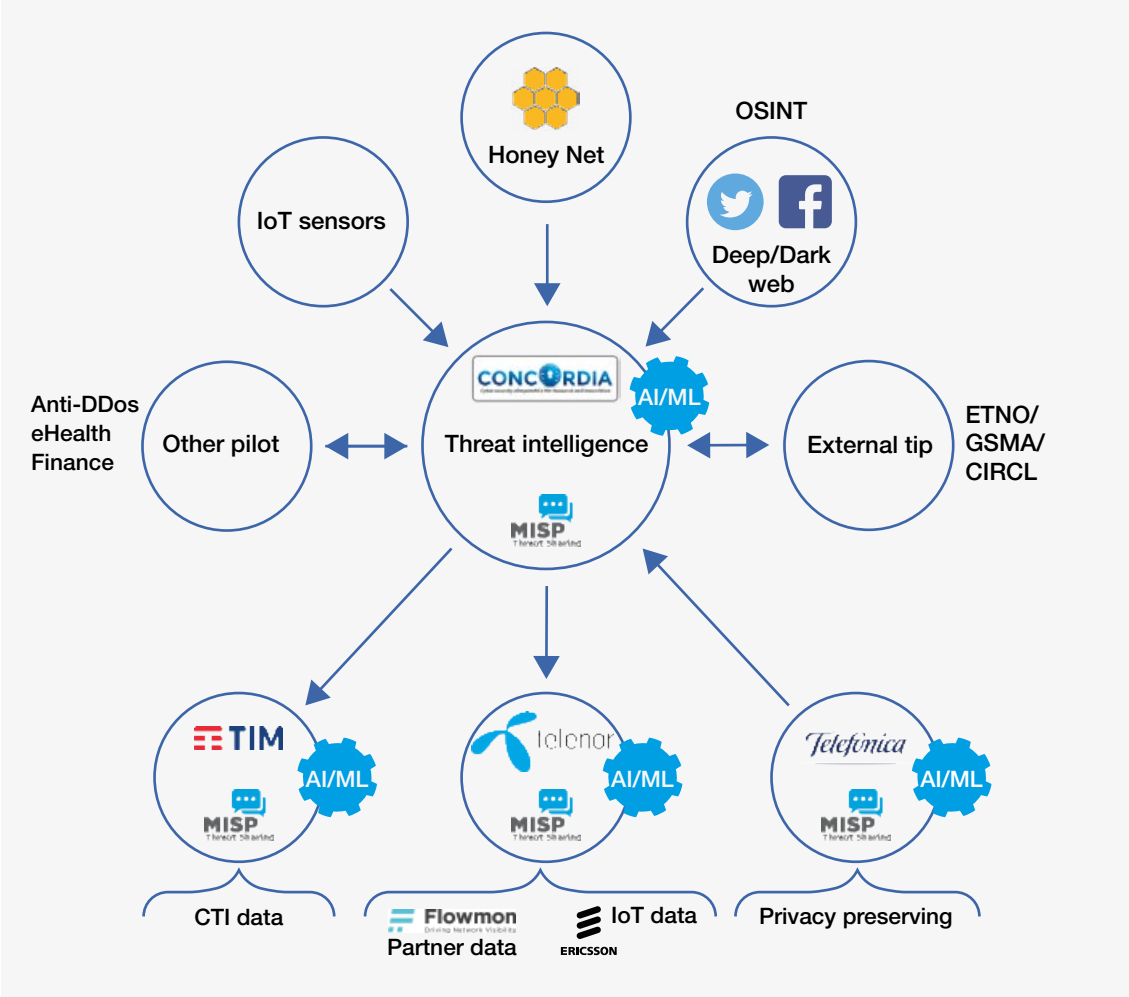


CONCORDIA is a H2020 European Union-funded project comprising 55 industry and academic partners. Its goal is to build a secure, resilient and trusted ecosystem. Information sharing is one of the most important aspects to address. This has resulted in the creation of "Threat Intelligence Platforms for Europe", which has enabled cross-sector (telecommunications, finance) collaboration in a wide variety of data sets and requirements.[15]

The respective project activity recognized that effective information sharing between different organizations in disparate sectors is not trivial and, as a result, a comprehensive plan was designed to overcome this. A mutual cyber intelligence sharing agreement was first drafted that allowed users of institutions to define the data they wanted to share, with whom, duration of the intelligence sharing, spatial and temporal characteristics (e.g. only shared in a specific country or for a specific period) and the definition of roles for accessing and controlling the information. This foundational model and way of working also allowed more mature organizations to then build federated machine learning approaches, leveraging the data sets of different participants, but preserving the privacy of data to enhance security.

The CONCORDIA platform is a way of joining up information from disparate data sources and sectors, thereby presenting a single view over Open-Source Intelligence (OSINT) information, based on financial services information and telecommunications-related data. The platform was built on existing, freely available open-source components, including the Malware Information and threat Sharing Platform (MISP) and the Incident Clearing House developed during the project "Advanced Cyber Defence Centre" (ACDC).[23] With this platform in place, different use cases can be more easily applied, which assist with the defensive posture of participants. This includes incident response and automated exchange of attack information.

FIGURE **CONCORDIA's Threat Intelligence Platforms**



Source: CONCORDIA (Cybersecurity Competence for Research and Innovation)

Recommendations

To address the barriers of better information sharing, the community puts forward the following recommendations. These are aimed at specific parts of the security ecosystem that can help address the barriers outlined in the report and help expediate some of the solutions identified.

Enterprise leadership

– Organizational leadership needs to treat cyber information sharing as a strategic capability and governed at a more senior level outside operational teams. With more senior governance and oversight, leadership can better build and resource information-sharing capabilities. This covers the investment in internal operational capabilities and technical platforms as well the necessary internal processes to engage external entities at a more systematic level. Leadership can significantly aid this process by providing assurance in a fragmented legal and policy landscape, including with appropriate oversight, potentially sharing what could be classified as sensitive and proprietary information.

Cybersecurity leadership

– Investigative authorities and information-sharing bodies should be exploring the potential applications for PETs in their operational partnerships and processes. More assessment work is required to identify new pilots to assess and applicability for cybersecurity and cybercrime use cases, especially in being able to facilitate more effective joint investigations. Regulators and government bodies, especially those with oversight of cybersecurity investigations and sharing bodies, need to issue guidance to entities on the applications, use and deployment of PET technology to accelerate their adoption.

– Information-sharing communities need to promote the use and potential of existing no-cost and open-source tools, contribute resources to the ongoing development and maintenance of those tools and actively participate in open-source software communities. Trusted and scalable cyber information sharing requires shared, flexible, trusted, widespread and low-cost technology underpinning it. The most effective way to rapidly develop cyber information sharing is to collectively advance the quality, flexibility and security of existing freely available technology.

– Work is required to make information-sharing frameworks and technical standards interoperable between jurisdictions and sectors. New models and enriched information-sharing frameworks will also need to be developed to deliver situational awareness in the face of increasingly complex technology environments. These need to be effective across national boundaries as well as throughout supply chains. Information-sharing initiatives should ensure that their data formats are open, easily available and widely shared to encourage interoperability and cross-sector collaboration. Having open formats allows for easy sharing of threat information between jurisdictions and sectors.

Policy and industry leadership

– Sector-specific guidance and frameworks should be created that map pre-existing privacy and rights-based principals, responsibilities, harms and remedies to the creation and management of cross-sector information-sharing efforts. By providing clear guidelines for ethical and responsible information sharing, existing communities will be able to rapidly innovate without being held back by uncertainty about possible harm.

– Legal and compliance meta-information-sharing efforts should be conducted to provide clarity about these concerns. This reduces the obstacles that stand in the way of information sharing. Ongoing active and public sharing of legal interpretation and compliance best-practices related to information sharing should be undertaken by existing sharing communities. This will reduce the initial resources required for organizations to evaluate the risk/rewards of taking on cyber information-sharing efforts as well as the ongoing resources required for information-sharing communities to ensure they maintain compliance in a fragmented and ever-shifting legal and policy landscape.

– More work is required to examine and promote effective incentives, positive and negative, for participation in the information-sharing ecosystem. The promotion of market and regulatory incentives to address the gaps, such as enhanced regulation, standards and especially the insurance market, might be required to promote and scale up information sharing through the cybersecurity ecosystem.

Research and operational community

– More research and deployments are needed to make AI and ML more operationally accessible as a defensive and information-sharing capability. More deployments will enable the community to start focusing on new threat intelligence frameworks and AI-based models. New sharing capabilities should be promoted that are able to share unstructured or loosely structured data, which can be fed into AI and ML pipelines.

Contributors

Lead Authors

David Balson
Director of Intelligence, Ripjar Technologies

William Dixon
Head of Future Networks and Technology, Centre for Cybersecurity, World Economic Forum

The Forum would like to thank the following for their contributions.

Arwa Alhamad
Cyber Security Enablement Director, stc

Fahad D. Alsehli
Threat Intelligence and Vulnerability Management Director, stc

Phillip Amann
Head of Strategy, European Cybercrime Centre

Yasser N. Alswailem
Cyber Security Vice-President, stc

Carlos Alvarez del Pino
Director of SSR Engagement, ICAAN

Daniel Bagge
Cyber Attache, National Cyber and Information Security Agency (Czech Republic)

Sandro Bucchianeri
Chief Security Officer, ABSA

Maya Bundt
Head, Cyber and Digital Solutions, Swiss Re

Belisario Contreras
Manager, Cybersecurity Program, Organization of American States (OAS)

Gabi Dreo Rodosek
Executive Director of the Research Institute CODE, Full Professor of Communication

Giulia Fanti
Assistant Professor of Electrical and Computer Engineering, Carnegie Mellon University

Samantha Kight
Security Operations Director, GSMA

Olaf Kruidof
Team Lead of Capability and Innovation, Europol

Kathrin Lotto
Head of Corporate Marketing, Duality Technologies

Sheetal S. Mehta
Group Chief Information Security Officer, WIPRO

Michael Meli
Chief Information Security Officer, Julius Baer

Arina Pazushko
Head of External Affairs, BI.ZONE

Neal Pollard
Chief Information Security Officer, UBS

Fernando Ruiz
Head of Operations, European Cybercrime Centre

Dimitry Samarstev
Chief Executive Officer, BI.ZONE

Rina Shainsky
Co-Founder, Duality Technologies

Maninder Singh Narang
Corporate Vice-President, Cyber Security and Governance, HCL Technologies

Bill Trent
Managing Director, Accenture Security

Joseph Trohak
Chief Information Security Officer, Scotia Bank

Seamus Tuohy
Director, Information Security, Human Rights Watch

Maria Vello
Chief Executive Officer, Cyber Defence Alliance

Ellison Anne Williams
Chief Executive Officer, Enveil

Bob Xie
Director Huawei Cybersecurity Transparency Centre, Huawei

Endnotes

1. https://www.weforum.org/reports/the-global-risks-report-2020
2. https://www.helpnetsecurity.com/2017/04/07/threat-intelligence-sharing-challenges/
3. https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/
4. https://www.thirdway.org/report/mentoring-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime
5. https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce
6. https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime
7. https://www.weforum.org/agenda/2018/09/moderate-approach-moderation
8. https://www.weforum.org/agenda/2020/01/5g-is-about-to-change-the-world-in-ways-we-cant-even-imagine-yet/
9. https://www2.banduracyber.com/resources/blog/importance-of-threat-intelligence-increasing-in-nist-cybersecurity-framework/
10. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf
11. https://www.ctin.us/site/isaos/
12. https://cybersecurityventures.com/jobs/
13. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020
14. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/pdf/G1823958.pdf?OpenElement12Ibid
15. Ibid Section VII
16. https://us-cert.cisa.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines.pdf
17. https://us-cert.cisa.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines.pdf
18. https://www.misp-project.org/15, https://thehive-project.org/16, https://github.com/TheHive-Project/Cortex17, https://github.com/certtools/intelmq
19. https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value
20. http://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf
21. HomomorphicEncryption.org
22. https://www.weforum.org/agenda/2019/10/cyber-crime-and-security-business/
23. https://www.misp-project.org/24acdc-project.eu/software/information-sharing-platformcentral-clearing-house/25, https://www.acdc-project.eu/

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