
# Paris Call for Trust and Security in Cyberspace:

## Multistakeholder Workstream on Public-Private Partnerships in Fighting Ransomware threats

---

*Compendium of Transnational Public-Private Partnerships Against Ransomware*

PARIS CALL
For trust and security in cyberspace

PARIS PEACE FORUM de PARIS sur la PAIX

PARIS CALL

For trust and security in cyberspace

# Paris Call for Trust and Security in Cyberspace:

## Multistakeholder Workstream on Public-Private Partnerships in Fighting Ransomware threats

---

*Compendium of Transnational Public-Private Partnerships Against Ransomware*

PARIS PEACE FORUM de PARIS sur la PAIX

## Executive summary

Over the past decade, ransomware has emerged as a prominent component of the global cyber threat landscape. This type of attack aimed at taking control of a target system in order to block, encrypt, steal and potentially delete its data is used mainly for immediate extortion purposes, requiring victims to pay a sum in exchange for the return of assets availability and confidentiality. While ransomware appeared in the end of 1980's, and are therefore not a new threat as such, their current incidence - estimated at 12% of data breaches in 2022 (IBM, 2022)- as well as their direct and indirect cost – 1.4 million $ per organization in 2021 (Sophos, 2022) are unprecedented. Another striking trend lies in the profile of the affected organizations, which are increasingly public institutions and critical infrastructure operators. Since the start of the Covid-19 pandemic, the health sector has become a prime target for threat actors, with 384 ransomware incidents recorded across 38 countries (CyberPeace Institute, 2022).

As a global phenomenon, the ransomware threat spares no industry or region across the globe the world and relies on a complex ecosystem - ranging from transnational organized crime to state-backed actors (Trellix, 2022). As with most challenges in cyberspace, which remains privately owned or operated for large parts, a global governance framework gathering all actors involved in the detection, prevention, reaction and repression of these should be sought. Ransomware attacks differ from other cyber malicious acts, however, as they are specifically based on blackmail, placing the victim in an even more active role when addressing these acts. In many cases, targeted private organizations don't know how to proceed when facing the disruption of their services and the risk of data loss or disclosure. The opportunity to pay the ransom requested, for instance, is still widely debated among stakeholders notwithstanding the cautions expressed by public authorities – as more than half of victims pay the ransoms according recent surveys (Kaspersky, 2021).

The dynamics of the phenomenon thus reinforce the need to achieve effective cooperation and common understanding between private and public actors. Public-Private Partnerships (PPPs), whose value has long been widely recognized in the cybersecurity field, have naturally been proposed as a key component of the response to ransomware. PPP are usually defined as an "*agreement/ cooperation/ collaboration between two or more public and private sectors and has developed through history in many areas*" (ENISA, 2018). While most actors agree on the usefulness of such a broadly defined action pattern, discrepancies remain between public authorities and the stakeholder community on what is concretely expected of each party.

Starting from this premise, the *Paris Call for Trust and Security in Cyberspace* has launched a workstream aimed at informing the intergovernmental work of the Working Group n°3 of the Counter Ransomware Initiative by providing a global,

multistakeholder lens. This workstream brought together representatives from the public sector, industry and civil society for a round of discussions initiated in mid-2022, where participants agreed on the drafting of the present compendium of existing global initiatives aimed at fighting ransomware threats through PPP cooperative models. The restitution of the current "state of play" was considered a necessary prerequisite to further discussions between communities toward the identification of replicable good practices for each stage of action.

Participants identified a substantial number of initiatives with a global or regional scope that rely on PPP cooperative models - suggesting broad adhesion to the idea that PPPs in the fight against ransomware are not only useful in the domestic context, but also at the supranational level. The existence of regional initiatives alongside initiatives with a worldwide scope suggest that the ransomware threat, while being a global phenomenon, is in part underpinned by local dynamics that deserve to be addressed more specifically.

A classification of these initiatives has been attempted on the basis of the nature of the goal pursued - which generally correlates with the mandate of the public organization(s) involved in the PPP. Since ransomware is primarily associated with cybercrime, the majority of existing initiatives are aimed at facilitating investigations as part of law enforcement activities (e.g. INTERPOL's Gateway Project, World Economic Forum's Partnership against cybercrime). A substantial number of initiatives also aim to provide policy and strategy recommendations for stakeholders, based on a prior identification of the gaps at this level as well as threat analysis (e.g. Ransomware Task Force, ENISA Working Group on Cyber Threat Landscape). Finally, a smaller number of initiatives focus on awareness raising and user empowerment by proposing guidance and tools in the event of a ransomware attack, which in turn facilitate investigations (e.g. No More Ransom Project).

The reconstitution of this landscape provides a baseline for building on what already exists, with a view to identify potential synergies and redundancies between initiatives, as well as gaps that are not currently addressed. In line with the feedbacks often expressed for cybersecurity PPPs at the domestic level, it appears for instance that the asymmetry in information sharing between partners of a different nature is still an obstacle to the full effectiveness of supranational initiatives. Continuing this work would provide an accurate picture of stakeholders' needs, which could then be addressed by drawing on good practices identified over the long term.

The participants of the workstream hope that this effort will effectively support the work of the Counter-ransomware initiative toward a global, comprehensive action against this ransomware threats. They will provide Working Group n°3 with their full report before the annual meeting of the Counter Ransomware Initiative, and will offer

participating States to exchange on the first outcomes of their work during a high-level roundtable in the framework of the 5th edition of the Paris Peace Forum, on November 11-12.

# Introduction

Launched in 2018 during the first edition of the Paris Peace Forum, The Paris Call for Trust and Security in Cyberspace is a global, multistakeholder initiative to improve trust, security and stability in cyberspace. The Paris Call is now gathering 1,200 supporters including 80 Governments, 700 companies and 350 organizations from the civil society around 9 core principles and a shared ambition of advancing common norms to defend a free, open and secure cyberspace.

Following the takeover of the initiative's informal secretariat by the Paris Peace Forum, the Paris Call community has launched three new workstreams starting June 2022 - building on the successful experience of the 2020-2021 working groups and their key deliverables. The workstream on "*Public-private partnerships in fighting ransomware threats*" was launched to cooperate with the Counter Ransomware Initiative (CRI). The CRI is an intergovernmental effort launched in 2021 to tackle ransomware in a comprehensive and global manner, gathering over 30 countries to date. This compendium is a contribution from the Paris Call community to the work of the CRI's working group #3 on public-private partnerships with a multistakeholder lens. This work is also fully in line with one of the main purposes of the Paris Call, which is to foster collaboration among all stakeholders from the public and private sectors on the most pressing cyber-related issues and stands as a proof of interest for multistakeholder inclusion in cyber international norm-making and policy.

This compendium is aimed as a resource to gain a better appreciation of the global state of play regarding public-private partnerships in the fight against ransomware. Such work is a precondition for identifying gaps and contemplating potential synergies in this field. The collection of information was facilitated by the sound expertise and experience of the participants in global public-private partnerships against ransomware, both at the national and supranational level.

The compendium has been divided in three sections to give a comprehensive and integrative overview of existing initiatives, following a finalist approach which focuses on main purposes and outputs of included initiatives - which are most of the time in line with the core mandate of the public organizations involved in the partnership:

I) Policy and Strategy
II) Law Enforcement Cooperation
III) User Empowerment

The initiatives were then classified according to their geographic scope - global or regional - considering the number of initiatives hosted by regional public organizations. The existence of many regional PPPs may suggest, beyond an opportunistic dimension,

that many stakeholders adhere to the idea that certain local dynamics should be the object of actions with a narrower scope, in parallel or even in collaboration with global initiatives.

The discussions conducted in 2022 finally allowed the Paris Call's community to share some lessons learned in this area, which will be outlined at the conclusion of this document as the basis for a prospective agenda of work in the longer term.

## I) Policy & Strategy

From prevention to resilience, an efficient fight against ransomware should rely on a clear, multi-layered and actionable framework that clarifies strategy and responsibilities for both public and private actors. Involving all stakeholders from the conception stage to define strategies, but also possible requirements of a public binding framework is instrumental in preventing gaps in regulation and increases the chances of rapid and efficient implementation. Furthermore, such inclusion helps in raising awareness among all actors on the objectives, constraints and field realities of the others. Public and private sectors also have complementary threat analysis capabilities that allow whose combination supports the development of policies in line with the reality of the ransomware phenomenon.

Several public-private partnerships have thus been developed across the Globe to design or inform the design of comprehensive strategies with different levels of implementation for a coordinated action among all key players of the cyber ecosystem. Such partnerships especially focus on the conception phase, leveraging on the experience of diverse constituencies to produce actionable recommendations and develop effective and systematic solutions to counter ransomware.

### A) Global scale

#### Ransomware Task Force

*https://securityandtechnology.org/ransomwaretaskforce/*

| | |
|---|---|
| **Main aim** | Uniting and building trust between key stakeholders across industry, government, and civil society, to innovate new solutions, break down silos, and find effective new methods of countering the ransomware threat. |
| **Date of Launch** | 2021 |
| **Host organization** | Institute for Security and Technology (Non-Governmental Organization) |
| **Geographical Scope** | Global, with an emphasis put on the United States. |

| | |
|---|---|
| **Outputs** | The Ransomware Task force has produced policy and strategic recommendations to be implemented by public authorities or organization from the private sector. In April 2021, the Ransomware Task Force launched its seminal report, " Combating Ransomware: A Comprehensive Framework for Action". The product of over 60 experts from industry, government, law enforcement, civil society, and international organizations, the report provided 47 specific and actionable recommendations and advocated for a unified, aggressive, comprehensive, public-private anti-ransomware campaign. The Ransomware Task force is now tracking progress against each of these recommendations and has launched several multistakeholder working groups on several priority issues:<br>• The Blueprint for Ransomware Defense focuses on the most critical cybersecurity controls that small and medium enterprises can adopt to counter ransomware threats.<br>• A cryptocurrency working group reflects on how to disrupt the financial side of ransomware.<br>• The cyber insurance working group discuss approaches for how the insurance industry can help move the needle on combating ransomware.<br>• An incident response reporting network is working to centralize advice, materials, and resources for victims, and promote information sharing between victims, governments, and other entities.<br>• An industry working group aspires to enhance increase efforts to share information with victims, with the goal of reducing the magnitude of ransomware incidents. |
| **Institutions and partners involved** | *Public Sector*: Jefferson County - Colorado; (National Governors Association); New York Department of Financial Services (NYDFS); Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3); U.K. National Crime Agency (NCA); U.S. Cybersecurity and Infrastructure Security Agency (CISA); U.S. Federal Bureau of Investigation (FBI); U.S. Secret Service (USSS).<br><br>*Private Sector*: a16z; Amazon Web Services; Aspen Digital; Banco Santander; Bank of America; Blackbaud, BlueVoyant; CFC Underwriting; Chainalysis; CipherTrace; Cisco; Citrix; Coveware; CrowdStrike; Cybereason; CyberArk; Datto; Deloitte; Ernst & Young; FireEye; Google; Mayer Brown; Mandiant; Krebs Stamos Group; McAfee; Microsoft; Palo Alto Networks; Rapid7; Recorded Future; Redacted; Red Canary; SecurityScorecard; Stratigos Security; Team Cymru.<br><br>*Civil society*: Aviation ISAC; Center for Internet Security; CyberPeace Institute; Cyber Threat Alliance; Cybersecurity Coalition; K12 SIX; The Shadowserver Foundation; Third Way; University of Oxford. |

## FIRST – Forum on Incident Response and Security Teams

*https://www.first.org*

| | |
|---|---|
| **Main aim** | FIRST aspires to bring together incident response and security teams across the world for a safer cyberspace, by fostering more efficient collaboration based on a strong trust and common language at the global level. |
| **Date of Launch** | 1990 |
| **Host organization** | N/A (Non-Governmental Organization) |
| **Geographical Scope** | Global |
| **Outputs** | To achieve its purpose, FIRST provides platforms, means and tools for incident responders to always find the right partner and to collaborate efficiently, support trainings and engage with relevant stakeholders, in technical and non-technical communities to ensure a favorable policy and governance environment for the collaboration between incident responders. While all of these missions contribute to the overall improvement of the fight against ransomware, FIRST has established a Multistakeholder Special Interest Group specifically aimed to foster collective action among the FIRST constituents, peer security organizations, and other groups who are focusing on the Ransomware Response, mitigation, remediation, investigation, and prevention. The group missions would include collecting material to enable a "one-stop shop" for any organization seeking the best ransomware help and producing international policy recommendations. |
| **Institutions and partners involved** | The Multi-Stakeholder Ransomware Special Interest Group would include some of the 652 emergency response teams which are member of FIRST, coming from public sector, industry and civil society across 101 countries. This effort would also be supported by two major industry-led coalitions with a global scope: the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group. |

## B) Regional scale

# OAS Cybersecurity Programme

*https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp*

| | |
|---|---|
| **Main aim** | Overseen by the Interamerican Committee against Terrorism, the Organization of American States' Cybersecurity Program aims to support the Member States of the organization in building technical and policy-level cybersecurity capacities, with the larger goal to ensure an open, secure, and resilient cyberspace throughout the Western Hemisphere. |
| **Date of Launch** | 2004 |
| **Host organization** | Organization of American States (OAS) (Public International Organization) |
| **Geographical Scope** | Americas |
| **Outputs** | To achieve its purposes, the OAS' Cybersecurity Programme has partnered with a number of key organizations from the stakeholder community for a broad range of missions, from threat analysis to strategy proposal and design of tools and trainings. In March 2022 for instance, the Organization and the cybersecurity company Trend Micro partnered to release a threat analysis report which devotes a large section to the threat of ransomware in Latin America and the Caribbean. |
| **Institutions and partners involved** | *(*The cyber partnerships with the OAS appear to be much more of a bilateral nature than truly multi-stakeholder)*<br><br>*Private Sector*: Amazon Web Services; Cisco; Citi; Meta; Microsoft; Trend Micro; Twitter.<br><br>*Civil Society*: Florida International University; Global Forum on Cyber Expertise; University of Oxford; World Economic Forum.<br><br>*Other*: Internet Corporation for Assigned Names and Numbers. |

# ENISA's Ad-Hoc Working Group on Cyber Threat Landscapes

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

| | |
|---|---|
| **Main aim** | As a long-time promoter of public-private partnerships in the cyber field, the European Union Agency for Cybersecurity (ENISA) itself has decided to draw on the expertise of the stakeholder community by launching a working group to feed ENISA's threat analysis work with reliable and accurate data, with the broader goal of supporting policy makers and practitioners. |
| **Date of Launch** | 2019 |
| **Host organization** | European Union Agency for Cybersecurity (Public International Organization) |
| **Geographical Scope** | Europe |
| **Outputs** | In 2022, the Working Group has contributed to the drafting of the ENISA Threat Landscape for Ransomware Attacks, which bring new insights on the current dynamics of the ransomware phenomenon through mapping and studying ransomware incidents from May 2021 to June 2022. The report also put forward several recommendations to build resilience against such attacks and to mitigate their impact. |
| **Institutions and partners involved** | *Private sector*: Accenture; cudeso.be; CYBHORUS; Exploit Labs GmbH; FalconForce; F-Secure; EnergiCERT; Kaspersky; McAfee; Nestle; NTT-CERT; Palo Alto Networks; PwC; SAP; SentinelOne.<br><br>*Civil Society*: Czech Technical University in Prague; University of Piraeus; University of Oslo; University of Piraeus; Stichting CyberDefcon Netherlands Foundation. |

## II) Law Enforcement Cooperation

Although the evolution of ransomware threats is now raising the issue of their impact on international peace and security, most ransomware situations fall under the realm of cybercrime and law enforcement cooperation. National authorities as well as relevant regional or international organizations have made tremendous progressed over the last 10 years in dismantling the criminal networks behind this phenomenon.

To facilitate their investigations and operations, law enforcement authorities can call upon the private sector through the traditional channel of vertical information sharing requests. However, partnerships between supranational police organizations and the private sector are becoming more sustained and permanent. Multistakeholderism is now a crucial element of the strategy of agencies such as INTERPOL and Europol, both in terms of threat analysis, crime identification, and operational support to investigations and operations. These partnerships, which mainly take the form of bilateral cooperation agreements or involvement in dedicated structures, have notably led to several operational successes in recent years leading to the dismantling of ransomware gangs.

### A) Global scale

### INTERPOL Gateway Framework

| | |
|---|---|
| **Main aim** | INTERPOL recently took a step forward in operational collaboration with the stakeholder community with the adoption by the INTERPOL General Assembly of the "Gateway" legal framework. Based on the understanding that law enforcement needs to work closely with the private sector where the majority of data and expertise lies in relation to cybercrime as well as on previous experience of collaboration with the stakeholder community since 2016, this framework enables INTERPOL to share information with private sector companies with which it has signed legal arrangements, to receive up-to-date cybercrime data from private partners from different sectors. These partners also share their expertise on recent trends and provide technical assistance for law enforcement agencies. The Gateway project therefore establishes a unique channel for the private sector to respond to requests for intelligence. |
| **Date of Launch** | 2019 |
| **Host organization** | INTERPOL (Public International Organization) |
| **Geographical Scope** | Global |
| **Outputs** | The new partnership framework led to several operational success over the past years. In late 2021 for instance, the arrest of six Clop ransomware gang members in Ukraine, following an international law enforcement operation code named "Operation Cyclone", was facilitated |

| | |
|---|---|
| | by the threat intel provided by Trend Micro, CDI, Kaspersky Lab, Palo Alto Networks, Fortinet and Group-IB. |
| **Institutions and partners involved** | *Private sector*: CDI; Fortinet; Group-IB; Kaspersky; Palo Alto Networks; Trend Micro; |

## INTERPOL Global Complex for Innovation

| | |
|---|---|
| **Main aim** | Before the adoption the Gateway framework, INTERPOL had already put the collaboration with the stakeholder community as a central element of its strategy, leading in particular to the opening of the INTERPOL Global Complex for Innovation (IGCI) in Singapore. This research and development facility, entrusted with threat analysis, identification of cybercrimes and criminals, innovative training and operational support, relies on partnerships with stakeholders at several levels. While companies provide most of IGCI's departments with seconded experts, a specific unit – the Cyber Fusion Center (CFC)– is truly dedicated to advancing multistakeholderism in the fight against cybercrime. The CFC has been established as a global platform where law enforcement and the private sector work together to gather and analyze all available information on criminal activities in cyberspace, then to develop innovative operational responses both prevent crime and aid in the identification of criminals, seeking to bridge the gaps that existed previously in such collaborations. |
| **Date of Launch** | 2014 |
| **Host organization** | INTERPOL (Public International Organization) |
| **Geographical Scope** | Global |
| **Outputs** | The Cyber Fusion Center has permitted a close monitoring of the cybercrimes - including ransomware attacks - at the regional and global scale, such as the surge of ransomware attacks that targeted hospitals since the start of the Covid-19 pandemic. One of the most striking achievements of this effort in recent years has been the Operation Quicksand (Goldust), which– under the supervision of the Cyber Fusion Center - led in 2021 to the arrest of 7 persons after a four-year effort involving 19 law enforcement agencies across the globe. The individuals arrested are suspected of carrying out tens of thousands of ransomware infections and demanding more than 200 million euros in ransom. |
| **Institutions and partners involved** | *Private sector*: Barclays; Cyber Defense Institute; Kaspersky ; LAC ; NEC ; SECOM ; TNO ; Trend Micro.<br><br>*Civil Society*: Univeristy of South Australia; University of Waikato, New Zealand. |

## Partnership Against Cybercrime

*https://www.weforum.org/projects/partnership-against-cybercime*

| | |
|---|---|
| **Main aim** | The World Economic Forum, whose core mission is to advocate for public-private partnerships, launched the Partnership Against Cybercrime to explore ways to amplify public-private collaboration in cybercrime investigations at the global level and initiate a paradigm shift in how to collectively address the growing impact of cybercrime. |
| **Date of Launch** | 2020 |
| **Host organization** | World Economic Forum (international non-governmental organization) |
| **Geographical Scope** | Global |
| **Outputs** | After a seminal report in November 2020, the Partnership is now striving to implement key recommendations by promoting joint research and operations processes to support and facilitate operational public-private cooperation to disrupt cybercrime. In 2022, the partners work on the development of a cybercrime ATLAS, to map cybercriminal ecosystem in a comprehensive manner. Eventually, the project aims to provide information to help senior executives make effective resourcing and targeting decisions about cyberthreats and support legal authorities with high-quality, actionable intelligence to increase the efficiency of cybercrime investigations. |
| **Institutions and partners involved** | *Public International Organization:* Council of Europe; Eurojust; European Commission; Europol; INTERPOL; World Bank.<br><br>*Public Sector*: Israel National Cyber Directorate; Ministry of Communications and Digitalisation of Ghana; UK National Crime Agency; US Department of Justice; US. Federal Bureau of Investigation; US Secret Service.<br><br>*Private Sector*: Accenture; Amazon; Banco Santander; Bank of America; Chainalysis; Check Point Software Technologies; Cisco; Cloudflare; Constella Intelligence; Credit Suisse; Dell Technologie; Deloitte; DXC Technology; EY; Fortinet; HCL; KPMG; Mastercard; Microsoft; Palo Alto Networks; Paypal; PwC; SpyCloud; Standard Chartered Bank; Trafigura Group; UBS; Wipro; Zurich Insurance Group.<br><br>*Civil Society*: Carnegie Endowment for International Peace; Cyber Defence Alliance; Cyber Threat Alliance; FIRST; Global Forum on Cyber Expertise Foundation; NCFTA.<br><br>*Other*: SWIFT. |

## B) Regional Scale

# Europol's European Cybercrime Center (EC3)

*https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3*

| | |
|---|---|
| **Main aim** | A decade ago, the European Union has established the European Cybercrime Center (EC3) under the Europol's umbrella, qualified by the 2013 EU Cybersecurity Strategy as the focal point in the fight against cybercrime at the continental level. The center is aimed to provide cybercrime intelligence and analysis, produce strategic analysis, provide high level technical forensic, contribute to capacity building activities and eventually support investigations and operations of Member States on cybercrime. To achieve its objectives, the EC3 was conceived as a hub to foster collaboration between law enforcement agencies and the private sector, particularly in terms of information sharing. Alongside the broad range of operational partnerships concluded with academia and the private sector, the EC3 has launched three multistakeholder advisory groups with a view of getting a clear overview of the needs and priorities for three major industrial sectors (internet security, financial services and communication providers) in the context of cross-border fight against cybercrime. |
| **Date of Launch** | 2013 |
| **Host organization** | Europol (Public International Organization) |
| **Geographical Scope** | Regional |
| **Outputs** | While few evidences are available regarding the precise extent to which the private partners cooperate with Europol for its investigations and operations, members of the advisory groups on internet security supported 8 major cross-border cybercrime operations in 2018, 2 of them at least targeting ransomware crimes. The advisory groups also contribute to the drafting of the annual EC3's Internet Organised Crime Threat Assessment, whose recent editions offer a detailed analysis of ransomware phenomenon dynamics and the ecosystem behind it. |

| | |
|---|---|
| **Institutions and partners involved** | *Public international organizations:* European Central Bank; EU DG Connect; EU DG Home.<br><br>*Private Sector*: ABI Lab; Aconite Internet Solutions; Akamai; American Express; Avast; Bank of America; Barclays; Belgacom; Betaalvereniging Nederland; BNP Paribas; Bitdefender; Broadcom; Bitsight Technologies ; Check Point; CISCO ; Citi Bank; Cloudflare; Coinbase; Crowdstrike; Danske Bank; Elisa; ESET ; Ericsson; Fire Eye ; Fox-IT ; Fraunhofer FKIE ; FS-ISAC; F-Secure ; GroupIB ; Grupo Santander; HSBC; ING Bank; Kaspersky ; KPN; Liberty Global; Mastercard; McAfee ; Microsoft ; Mnemonic ; NCSC ; NTT Security; OpenXChange; Orange; Palo Alto Networks ; Paypal; Portugal Telecom; Qintel ; S21Sec ; Shadowserver ; Standard Chatered; Telefonica; Telekom Slovenije; Telenor; Trend Micro; UBS; Visa; Vodafone; Western Union.<br><br>*Civil Society*: Fraunhofer Institute for Communication, Information Processing and Ergonomics; Banking and Payments Federation Ireland; European Banking Federation; GSMA; NLD Digital; RIPE NCC; Ukrainian Interbank Payment Systems Members Association; World Economic Forum<br><br>*Other*: CENTR, SWIFT |

## III) User empowerment

Ransomware attacks place the victim in a unique position that relates to their ability to choose and act when facing the ransom demand. This choice can therefore lead, on the one hand, to the enrichment of criminal networks and the prolongation of this lucrative phenomenon, or on the other hand to the definitive loss of encrypted data with sometimes very extensive consequences for the victims. In the absence of a consistent doctrine and accessible assistance, the victim is faced with an even more difficult choice.

User empowerment is therefore a crucial part of the fight against ransomware, which should be based not only on clear guidance but also on innovative solutions to enable victims to get out of this complex dilemma. The stakeholder community has significant resources in this regard, from awareness raising campaigns to support frameworks, which could help to give weight to the requirements issued by public authorities. Close cooperation between public and private actors in this regard would especially increase the larger resilience of the ecosystem, tackle the human factor dilemma, and could subsequently diminish the incentives for ransomware attackers to act.

### A) Global Scale

#### No More Ransom Project

*https://www.nomoreransom.org*

| | |
|---|---|
| **Main aim** | The No More Ransom project, launched by Europol, the Dutch Police, Kaspersky and McAfee is an innovative initiative focused on helping victims of ransomware decrypt their data for free, in particular by providing available decryption tools, clear guidance and the right focal points among national or international authorities. |
| **Date of Launch** | 2016 |
| **Host organization** | N/A |
| **Geographical Scope** | Global |
| **Outputs** | After 6 years of activity, No More Ransom provides 136 free tools for 165 ransomware variants with the participation of over 150 public and private partners, and has helped 1.5 million people successfully decrypt their devices without needing to pay the criminals. The portal is available in 37 languages in order to better assist victims of ransomware across the globe. |

| | |
|---|---|
| **Institutions and partners involved** | *Public international organizations:* Europol<br>*Public Sector*: Belgian Federal Police; Dutch Police; French Police; Korea Internet & Security Agency; Romanian Police.<br><br>*Private Sector*: Amazon Web Services; Avast; Baraccuda; Bitdefender; Checkpoint; Cisco; Cycraft; Eleven Path; Emisoft; ESET; F-Secure; Kaspersky; McAfee; Tesorion; Trend Micro.<br><br>*Civil Society*: Bleeding Computer; CERT.PL. |

## Conclusion

The number of initiatives identified in this compendium shows a clear endorsement by the cyber community of the relevance of public-private partnerships the global threat of ransomware. The outcomes of the above-mentioned initiatives can only strengthen this argument. However, this finding does not imply that existing transnational PPPs have achieved optimal cooperation and efficiency to date. The workstream participants' long-standing involvement in this type of collaboration, including in the initiatives collected here, provided an opportunity to discuss some of the gaps they have experienced in the process. In particular, participants noted that "Two Way" information sharing is key but was not systematically carried out. The fragmentation of the favorable legal, conceptual, and political environment was also identified as a frequent barrier to effective collaboration between partners.

The fifth edition of the Paris Peace Forum will provide an opportunity to further discuss these points and to compare the experiences of participants with those of a wider range of critical actors in the global efforts against ransomware. The conclusions of this high-level debate should make it possible to lay the foundations for a forward-looking work agenda as part of this workstream. In particular, it will allow to confirm or not the relevance of (i) working on the development of recommendations for transnational PPPs based on an in-depth investigation of the functioning of existing initiatives and (ii) to investigate possible gaps and synergies in the current initiative landscape, as suggested by the workstream's participants over the past months.

# Paris Call for Trust and Security in Cyberspace:

## Multistakeholder Workstream on Public-Private Partnerships in Fighting Ransomware threats

*Compendium of Transnational Public-Private Partnerships Against Ransomware*

PARIS CALL
For trust and security in cyberspace

PARIS PEACE FORUM de PARIS sur la PAIX


### Contact

**Jérôme Barbier**

Head of Outer Space, Digital & Economic Issues
Policy Department | Paris Peace Forum

jerome.barbier@parispeaceforum.org

**Pablo Rice**

Cyberspace Governance Policy Officer
Policy Department | Paris Peace Forum

pablo.rice@parispeaceforum.org