Council of the
European Union

Brussels, 24 October 2022
(OR. en)

13938/1/22
REV 1

LIMITE

CYBER 336
COPEN 361
TELECOM 420
JAIEX 92
RELEX 1410

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	13787/22 REV 1
Subject:	International Counter Ransomware Initiative 2022 draft Joint Statement and the letter from the Commission to Permanent Representatives Committee

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (07.11.2022)

Delegations will find in the Annex the revised International Counter Ransomware Initiative 2022 draft Joint Statement and the letter from the Commission to the Permanent Representatives Committee.

International Counter Ransomware Initiative 2022
DRAFT Statement

The members of the International Counter Ransomware Initiative (CRI)—Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Croatia, Czech Republic, Dominican Republic, Estonia, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Poland, Republic of Korea, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, United Arab Emirates, United Kingdom, United States, and Ukraine, and the EU—met in Washington, DC on October 31–November 1, 2022. Previously participating states welcome Belgium as a new CRI member.

At the Second CRI Summit, members re-affirmed our joint commitment to building our collective resilience to ransomware, cooperating to disrupt ransomware and pursue the actors responsible, countering illicit finance that underpins the ransomware ecosystem, working with the private sector to defend against ransomware attacks, and continuing to cooperate internationally across all elements of the ransomware threat.

The work of the CRI supports the implementation of the agreed upon UN normative framework for responsible state behavior in cyberspace, specifically the norm that States should cooperate "to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and

implement other cooperative measures to address such threats." The joint efforts of the CRI partners are also directly contributing to the implementation of the consensus conclusions and recommendations of the UN Expert Group to Conduct a Comprehensive Study on Cybercrime.

We are committed to using all appropriate tools of national power to achieve these goals and jointly committed to the following actions in support of this endeavor. We intend to:

- Hold ransomware actors accountable for their crimes and not provide them safe haven.
- Combat ransomware actors' ability to profit from illicit proceeds by implementing and enforcing anti-money laundering and countering the financing of terrorism (AML/CFT) measures, including "know your customer" rules, for virtual assets and virtual asset service providers.
- Disrupt and bring to justice ransomware actors and their enablers, to the fullest extent permitted under each partner's applicable laws and relevant authorities.
- Collaborate in disrupting ransomware by sharing information, where appropriate and in line with applicable laws and regulations, about ransomware actors' misuse of infrastructure to launch ransomware attacks to ensure national cyber infrastructure is not being used in ransomware attacks.

Building our resilience to ransomware attacks requires effective policies and cooperation with trusted partners. CRI members are building a network of trusted partners to share and disseminate ransomware-related threat information to increase our collective resilience to ransomware attacks. To that end, a Counter Ransomware Task Force (CRTF) will be established to develop cross-sectoral tools and cyber threat intelligence exchange to increase early warning capabilities and prevent attacks, as well as consolidate policy and best practice frameworks among CRI members. The CRTF will produce public reports on tools, tactics, and procedures to improve awareness to global stakeholders, promote and encourage membership of the CRI, and improve cyber hygiene across the board. The CRTF will also consider a model for ongoing collaboration with key private sector partners, including the establishment of an ancillary industry chapter which would be actively engaged with the work of the CRTF.

CRI members are committed to taking action based on our collective knowledge, expertise, authorities, and capabilities to disrupt and degrade the ransomware ecosystem and hold accountable criminal actors. We intend to improve our comprehensive and holistic understanding of the strategies used by criminal actors and the means by which their malicious activity can be identified and addressed in respective jurisdictions to improve our tools, relevant authorities, and capabilities to disrupt. We commit to work together to prioritize disruption targets through a collective framework to leverage the breadth of authorities and tools available to pursue hard and complex targets more effectively. We intend to increase the number and impact of our disruption actions so that ransomware actors are stopped in their tracks.

The CRI is committed not only to protecting ourselves and each other from ransomware, but also to helping other countries protect and disrupt so that ransomware is unable to gain traction worldwide. To that end, we intend to share technical and threat information and provide protection and remediation recommendations as broadly as possible.

Taking decisive steps to counter illicit finance that often enables and underpins the profitability of ransomware will also be key to our collective success. We resolve to work to establish mechanisms for notifying financial institutions and virtual asset platforms of ransomware payments so that funds can potentially be seized once they land in ransomware actors' accounts. We commit to working together to promote AML/CFT controls, including KYC policies and procedures within the virtual assets ecosystem to prevent its use for illicit ransomware activity, such as through the implementation and enforcement of the Financial Action Task Force recommendations.

The private sector has a unique role to play in our counter-ransomware efforts, as their insights into the whereabouts and actions of ransomware actors from across the internet can effectively complement state capabilities in this realm. Private sector companies are often the victims of ransomware, and can be strong allies in defense and disruption. CRI members are working closely with the private sector to share information and set goals to prevent, reduce, and respond to ransomware threats. To further this collaboration, we have established a pilot information sharing platform to facilitate the exchange of information about ransomware actors and tools, tactics, techniques, and procedures amongst members and with the private sector. In addition, we will also develop a capacity-building tool to help countries utilize public-private partnerships to combat ransomware. We will continue to work together to develop additional ways to collaborate to combat ransomware with the private sector, taking into account concerns private sector companies may raise.

Diplomatic engagement continues to be an essential tool for the international community's fight against ransomware attacks. We are committed to continuing to work together not only as the CRI, but also with other partners committed to fighting the scourge of ransomware, which has the power to impact us all, including through the Paris Call for Trust and Security. CRI members plan to work with the full spectrum of stakeholders to drive focused regional efforts and advance this agenda in appropriate multilateral frameworks to ensure the global community's shared resolve and preparedness to defeat these threats. We are also committed to leveraging capacity building programs in order to strengthen resilience, improve disruption capabilities, increase law enforcement's capacities, and support the development of legal frameworks to combat ransomware in both CRI and other countries.

EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Directorate Digital Society, Trust & Cybersecurity
Unit H.2 for Cybersecurity and Digital Privacy Policy

Brussels, 21 October 2022

NOTE FOR THE ATTENTION OF THE PERMANENT REPRESENTATIVES COMMITTEE

SUBJECT: **Request for endorsement for the Commission to sign the *Joint Statement* on the *International Counter Ransomware Initiative* on behalf of the EU with 36 other countries**

***CONTACT POINTS*:** **Commission DG CONNECT Unit H2 Cybersecurity & Digital Privacy Policy**

DELETED

Head of Unit

DELETED

DELETED @ec.europa.eu

DELETED

Policy Officer

DELETED

DELETED @ec.europa.eu

REMARKS:

Context

The 2022 Summit of the Counter Ransomware Initiative will be hosted by the US (White House – National Security Council) on 31 October and 1st November 2022 in Washington. As an outcome of the event, the US propose the adoption of a joint statement to be signed by all members present. The summit aims to take stock of the work of the five working groups that have been established under the initiative launched one year ago. The five existing working groups of the Counter Ransomware Initiative are: Resilience, Diplomacy, Disruption, Countering Illicit Financing, and Public-Private Partnership.

The Counter Ransomware Initiative was formally kicked off by the US (White House – National Security Council) in October 2021 at the outcome of which about 30 members, including the EU, signed a joint statement[1] outlining focus areas of cooperation. Cooperation between the EU and US on countering ransomware falls within the ambition of the Joint Statement by President Biden and President von der Leyen of 24 March 2022[2], in committing the EU-US "partnership in the Counter Ransomware Initiative to disrupt ransomware groups and reduce related threats to our citizens and businesses". Moreover, a bilateral EU-US working group on ransomware group has been established following the agreement by Commissioner Johansson and the US Secretary of Homeland Security Mayorkas at the JHA in Lisbon in June 2021.

1 https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

2 https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/24/joint-statement-by-president-biden-and-president-von-der-leyen/#:~:text=We%20are%20united%20in%20our,brutal%20onslaught%20against%20its%20neighbor.

Besides the European Union, 16 Member States have been invited and are expected to take part to the 2022 Summit and to sign the joint statement (AT, BE, BG, HR, CZ, EE, FR, DE, IE, IT, LT, NL, PL, RO, ES, SE) as well as 20 other countries including Australia, Brazil, Canada, Dominican Republic, India, Israel, Japan, Kenya, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Republic of Korea, Singapore, South Africa, Switzerland, United Arab Emirates, United Kingdom, United States, and Ukraine.

Current process

On 30 September 2022, the Commission informed the Horizontal Working Party for Cyber Issues (HWPCI) of the Council about the preparation of the 2022 International Counter Ransomware Initiative Summit indicating that a draft joint statement was expected from the US. The draft joint statement was shared by the US (National Security Council) with CRI members on 8 October 2022 with a deadline for comments by Thursday 13 October 2022. The European Commission requested one extra day for comments. The draft statement was shared on 11 October with the HWPCI of the Council.

On 12 October, the Commission presented to HWPCI of the Council the draft Statement and timeline for negotiating the content of the Statement, which the signatories will subscribe as the outcome of the Summit. On 14 October, the HWPCI of the Council had discussions on the matter, Member States examined the text, expressed initial positions and a clear interest in the EU being represented. Subsequently, the HWPCI of the Council requested to launch an NBI procedure, and a note was submitted by the Presidency to the Permanent Representatives Committee to confirm the agreement for the Commission to enter into the negotiations on this joint statement. The meeting of the Permenant Representatives Committee took place on 19 October.

The Commission submitted comments to the US on 14 October, limited to linguistic changes.

Next steps

The US is in the process of consolidating all comments received and may circulate a revised version to CRI members (timing to be confirmed) before circulating the final version for approval via silent procedure before the meeting itself .

The Commission requests the Council to endorse the EU's subscription to the joint statement based on the draft joint statement in attachment. No further substantial changes are expected. The draft joint statement will be subject to further editorial or fine tuning on the spot. The Union position on the statement will then be expressed by Gerard de Graaf, Head of the EU office in San Francisco, in the absence of a member of the College at the event.

It should be noted that the joint statement does not pre-empt or prejudge our positions with respect to negotiations in parallel forums and does not create legal effects.