Council of the
European Union

Brussels, 24 October 2023
(OR. en)

14634/23

LIMITE

CYBER 261
COPEN 371
TELECOM 313
JAIEX 74
RELEX 1226

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	International Counter Ransomware Initiative 2023

Delegations will find in the Annex the International Counter Ransomware Initiative 2023 draft Joint Statement.

ANNEX

International Counter Ransomware Initiative 2023 (version circulated on 18 October 2023, with EU comments of 23 October incorporated)

DRAFT Joint Statement

International Counter Ransomware Initiative 2023 Joint Statement

The 50 members of the International Counter Ransomware Initiative (CRI)— Albania, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Colombia, Costa Rica, Croatia, the Czech Republic, the Dominican Republic, Egypt, Estonia, the European Union, France, Germany, Greece, India, INTERPOL, Ireland, Israel, Italy, Japan, Jordan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Papua New Guinea, Poland, Portugal, the Republic of Korea, Romania, Rwanda, Sierra Leone, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, the United States, Ukraine, and Uruguay —met in Washington, D.C. on October 31-November 1, 2023. Previously participating states welcomed Albania, Colombia, Costa Rica, Egypt, Greece, INTERPOL, Jordan, Papua New Guinea, Portugal, Rwanda, Sierra Leone, Slovakia, and Uruguay as new CRI members.

During the third CRI Summit, members reaffirmed 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.

Over the past year, this coalition has grown and built upon the commitments made at the second CRI Summit in 2022. Through unveiling operational tools, the International Counter Ransomware Task Force (ICRTF)—established at last year's Summit—began developing the platforms necessary for coordinating and disrupting ransomware at an operational level. By adding thirteen new members to the coalition, the Diplomacy and Capacity Building Pillar expanded the CRI's like-minded umbrella and incorporated capacity building efforts throughout all pillars and working groups of the CRI. The Policy Pillar led efforts to counter the business model that underpins the ransomware ecosystem. This included research on cyber insurance, victim behavior, seizure and confiscation of virtual assets, ransom payments, and best practices in incident reporting and information sharing. Throughout the year, the coalition sought to incorporate the private sector and integrate capacity building at every opportunity.

We remain committed to using all appropriate tools of national power to achieve these goals and jointly committed to the following actions in support of this mission.

CRI members intend to:

- Develop ransomware incident reporting mechanisms and encourage the private sector and general public to report all ransomware incidents and payments to responsible authorities
- Regularly share actionable information with the CRI members;
- Expand Policy Pillar projects to include new focus on the impact of discouraging ransom payments and explore the key policy issues that could have the most impact on the ransomware business model;
- Continue to expand CRI membership and push forward on operational and policy cooperation;
- Enhance cyber capacity building through mentorship of new members; and
- Provide tactical training and operational tools through the ICRTF to develop national capabilities to prevent ransomware attacks.

The experience of CRI provides an opportunity to further reshape the cyber environment by creating long-term cooperative approaches and common understandings of accountability in cyberspace, consistent with international law as well as state actions as embodied in the Framework for Responsible State Behavior in Cyberspace, endorsed by all United Nations member states.

Through the Policy Pillar, CRI members affirmed the importance of adopting strong and aligned messaging discouraging paying ransomware demands and leading by example: endorsing a statement that relevant institutions under our national government authority should not pay ransomware extortion demands. CRI members also agreed to implement the Financial Action Task Force (FATF)'s Recommendation 15 on the regulation of virtual assets and related service providers, which would help stem the illicit flow of funds and disrupt the ransomware payment ecosystem. CRI members also affirmed the importance of developing a ransomware incident reporting mechanism within their own jurisdiction, and sharing actionable information to strengthen our collective efforts to bring ransomware actors to task. The Policy Pillar also examined the role of the cyber insurance industry in ransomware, and committed to enhancing engagement with industry, as well as undertaking research into the importance of developing effective crypto asset seizure regimes.

Over the next year, the Diplomacy and Capacity Building Pillar will continue to expand the CRI's mentorship program and onboarding program. The Pillar will prioritize opportunities to educate potential new members about the Initiative, and it will develop tailored capacity building opportunities to match members' and potential new members' needs and requests.

Going forward, the ICRTF will build upon the successes of its inaugural year by operationalizing the tools and platforms developed by its members. Members will work toward attaining a comprehensive understanding of the ransomware threat by aggregating and sharing their information and exchanging knowledge through virtual seminars and labs. Members plan to create and share resources to build their national counter-ransomware capacity, working closely with the other pillars develop practical tools for governments to prevent, respond to, and recover from ransomware attacks, uplift cyber capabilities across the existing CRI membership and advocate new membership to those countries who will most benefit from what the CRI has to offer. The ICRTF will also continue to support transnational operations conducted by its members and collaborate with industry to target disruptive activities at key components of ransomware ecosystem, in recognition that ransomware is a cross-border and cross-sectoral threat that necessitates close collaboration across governments and sectors to be effectively combatted.

The third CRI Summit leveraged the expertise of like-minded partners, private sector participants, and capacity building experts to further reshape the cyber environment so members are better equipped to combat ransomware. Members from around the world reaffirmed our joint commitment to building out our toolkit for collective resilience to ransomware, cooperating to disrupt ransomware, and working together to curb the illicit money flow that ransomware actors rely upon. We are building capacity through long-term cooperative approaches and refining our understanding of accountability in cyberspace, bringing us one step closer to rooting out bad actors and responding with collective resolve. The members express their gratitude towards the countries who have taken on leadership roles in the CRI: US as Secretariat; Australia as lead of the ICRTF; Singapore and the United Kingdom as Policy Pillar leads; and Germany and Nigeria as Diplomacy and Capacity Building Pillar leads. Through the Initiative's annual Summit, as well as the dedicated work that is happening between each Summit, we commit to working together on a policy and operational level to counter ransomware threats and hold perpetrators of these vicious attacks accountable.