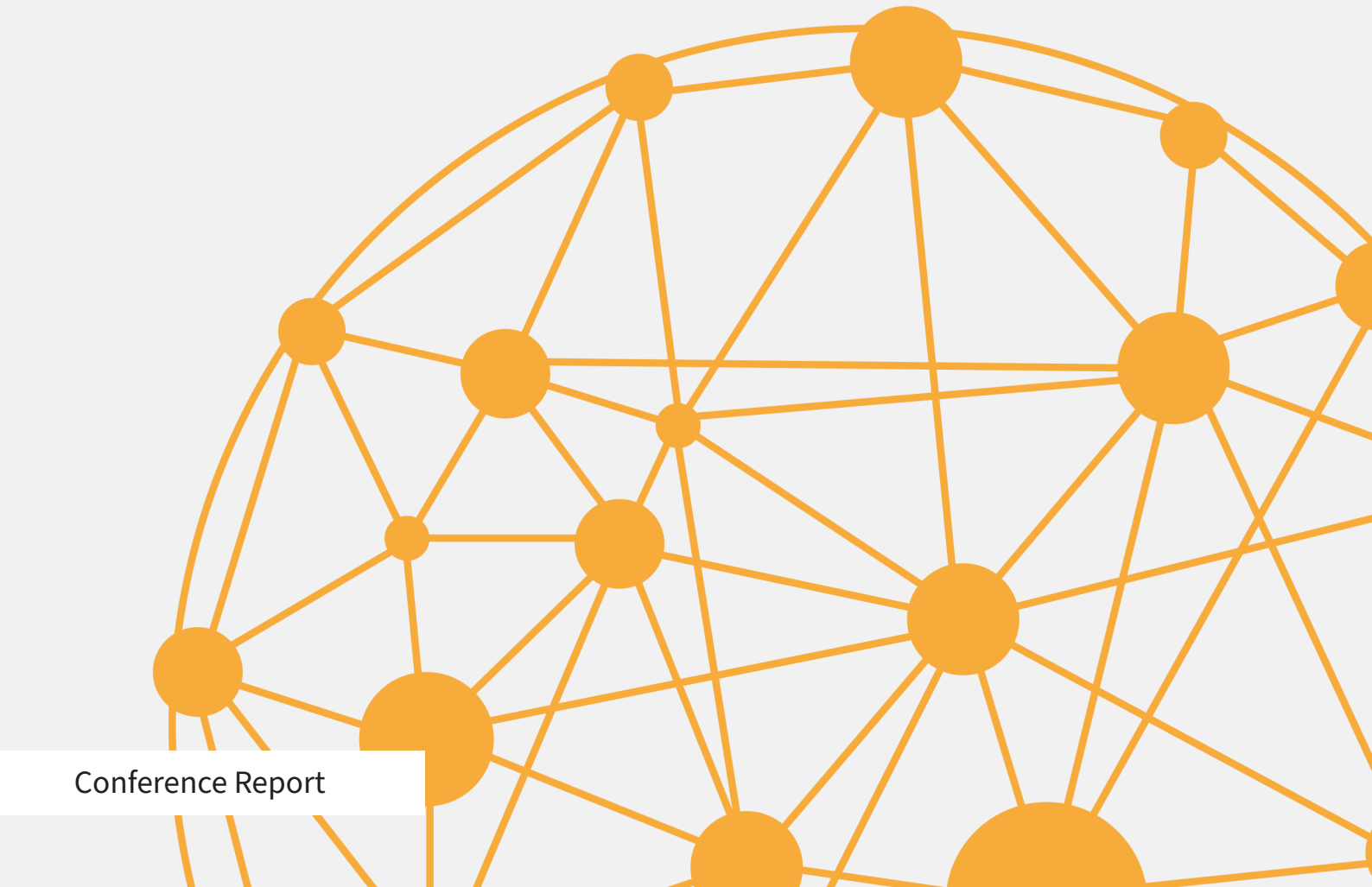
GLOBAL PARTNERSHIP FOR RESPONSIBLE CYBER BEHAVIOUR

RUSI

Conference Report

Decoding Emerging Threats: Ransomware and the Prevention of Future Cyber Crises

Louise Marie Hurel



Conference Report

192 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.

RUSI Conference Report, September 2023.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

PERMANENT MISSION OF ESTONIA TO THE UN

PERMANENT MISSION OF COSTA RICA TO THE UNITED NATIONS

RUSI

On 24 July 2023, RUSI and Estonia – with the co-sponsorship of the governments of Costa Rica and Vanuatu – organised a closed roundtable on 'Decoding Emerging Threats: Ransomware and the Prevention of Cyber Crises'. The event took place on the sidelines of the negotiations of the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies. The discussion gathered 30 participants (governmental and non-governmental organisations) at the Permanent Mission of Estonia to the UN for a dialogue on ransomware, crisis prevention and responsible cyber behaviour.

The first part of the dialogue discussed what constitutes the international peace and security threshold for ransomware incidents. The second part reflected on the implementation of existing norm that notes that states should respond to requests for assistance when facing a cyber incident. This report provides an overview of the main points raised during the workshop as well as recommendations for future dialogues.

In recent years, ransomware incidents have captured the attention of both developed and developing economies. While incidents vary in complexity, when successful, they can deliver nation-wide crippling effects. As many cases have shown, governments have become a particular target of many ransomware groups, leaving departments, critical infrastructures, essential services and entire local governments unable to function.

Within the context of the OEWG, several member states have highlighted the importance of recognising ransomware as an emerging threat in the context of international peace and security. While important, this also raises challenges, such as determining when and what qualifies as a ransomware incident beyond the criminal sphere.

The objective of the event was threefold:

- Share/reflect on lessons learned from responding to and recovering from ransomware incidents.
- Discuss how the OEWG's work should/could reflect such a threat.
- Examine how experiences of responding to and recovering from incidents could help shape future cooperative and coordinated responses.

While ransomware has been recognised in the 2023 Annual Progress Report (APR)[1] – a consensus report annually discussed and negotiated by member states

1. UN, 'Draft Annual Progress Report', A/AC.292/2023/CRP.1, 28 July 2023, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_27_July_2023.pdf>, accessed 8 September 2023. The final APR was still to be published online at the time of writing this report, however, the version presented by the Chair prior to the last day of negotiations already included ransomware – a reference that remained in the final version.

engaged in this process – one of the continuous challenges for the OEWG (and the future Programme of Action (PoA)[2]) is to understand how to go beyond adding new emerging threats to the list and effectively address them in a constructive manner within the scope of the UN First Committee.

During the discussions, the following indicators were considered when reflecting on when a ransomware incident could cross the international peace and security threshold: scale, scope and speed, impact, motivation and funding.

Equally, representatives discussed the implementation of norm 13(h)[3] on requests for assistance and how to foster coordination and collaboration to support ransomware recovery. The following priority areas emerged during the dialogue: ensure cross-government awareness of the criticality of the incident in a timely and effective manner; strengthen coordination among states providing and/or seeking to provide support to the victim state; and develop sustainable capacities for countries to proactively monitor and respond to incidents.

Overall, the workshop discussion illustrates that context-sensitive discussions can provide further understanding of the activities and challenges underpinning the practice of responsible behaviour in cyberspace by developed and developing countries as well as state and non-state actors. In exploring ransomware specifically, the dialogue engaged representatives in a detailed and practical assessment of lessons learned and the human, technological, contextual and procedural challenges involved in providing responses to large-scale incidents.

From Crime to International Peace and Security: When and Where to Draw the Line

Often ransomware is associated with criminal groups and activities. Criminal actors have made use of ransomware for multiple purposes such as financial gain, data theft and exfiltration, and disruption of operations and espionage, among others. However, as these groups have increasingly sought to disrupt public entities and critical services, additional considerations on what might

2. See UN, 'Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security', A/RES/77/37, 12 December 2022; UN, 'Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in The Context of International Security: Report of the Secretary-General', A/78/76, 18 April 2023.
3. See the 11 norms agreed by the UN Group of Governmental Experts in the field of information and communications technologies (ICTs) in the context of international security in 2015. UN, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, 22 July 2015.

differentiate the criminal and national security dimensions of ransomware require further attention. Countries such as Costa Rica[4], the US[5], the UK[6] and others have already highlighted the risk that ransomware poses to national security. During the workshop, other states, such as El Salvador and Switzerland, also noted the high priority of ransomware within the international agenda and their own domestic cyber threat landscapes respectively.

For the past two years, member states have reiterated the importance of ransomware incidents within the context of the OEWG. However, the fact that, despite widespread reference to it, ransomware was only referenced in this year's APR instead of last year's, is perhaps indicative that there are elements that still merit further discussion. As cases, victim countries and tactics continue to evolve, states should consider what distinguishes the criminal and the international peace and security dimensions of ransomware incidents.

During the first part of the discussion, member states and stakeholders were invited to reflect on what constitutes the international peace and security threshold for ransomware incidents. To kick off the dialogue, Costa Rica and Vanuatu shared their experiences of being at the forefront of disruptive and notorious ransomware incidents. Following that, other states and representatives engaged in the discussion, providing their own views on what should inform the delineation (or lack thereof) of the international peace and security threshold for assessing ransomware incidents.

During the first part of the dialogue, participants addressed the following questions:

- Incidents such as the one faced by Vanuatu and Costa Rica have shed important light on the disproportionate impact of ransomware on a national economy and government functions. From national experience, what is the internal 'tipping point' when the incident shifts from criminal/law enforcement issue to a national security issue?
- Based on those national experiences, what kinds of factors differentiate the prosecution of ransomware incidents within the criminal law from those that reach an international peace and security threshold?
- What are potential qualifiers that could support future OEWG discussions?

4. Ax Sharma, 'Costa Rica Declares National Emergency After Conti Ransomware Attacks', BleepingComputer, 9 May 2022, <https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/>, accessed 8 September 2023.
5. The White House, 'National Cybersecurity Strategy', March 2023, p. 17, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, accessed 8 September 2023.
6. HM Treasury Office of Financial Sanctions Implementation, 'Ransomware and Sanctions: Guidance on Ransomware and Financial Sanctions', <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135587/Ransomware___Sanctions_guidance__Feb_2023_.pdf>, accessed 8 September 2023.

International Peace and Security Indicators for Ransomware Incidents

The following indicators were highlighted by participants as potential determinants for differentiating the criminal scope from the national and international security scope of ransomware:

Scale, Scope and Speed

The first set of indicators raised by government representatives was scale, scope and speed. In the case of Costa Rica, for example, the fact that incidents hit 'hard and fast' with more than 20 ministries targeted, with nine of them becoming severely impacted, clearly showcases the disproportionate reach and disruptive effects that ransomware may bring about in the public sector. For Vanuatu, the incident, which took place less than a month after the new government had been elected, affected a wide range of government entities, all gov.vu email and domains, as well as reportedly leaving citizens 'scrambling to carry out basic tasks like paying tax, invoicing bills and getting licenses and travel visas'.[7]

Other participants noted that ransomware, although important, would be more clearly demarcated as an international peace and security issue when connected with critical infrastructure (CI) or disruption of essential services. Given the extensive references to CI in previous Group of Governmental Experts (GGE) and OEWG reports,[8] ransomware mitigation experiences would help states understand how CI norms are implemented, tested and challenged. It was also pointed out that ransomware incidents may raise questions related to the applicability of international law to cyberspace – for example, whether such an incident could entail a breach of sovereignty.

Such an evidence and experience-based dialogue on scale, scope and speed indicators highlighted the different levels of prioritisation of the threat by governments. States present at the event that have not been severely affected by ransomware noted that there is little incentive for them to treat ransomware as a national security threat by default. Rather they assess it on a case-by-case

7. *BBC News*, 'Vanuatu: Hackers Strand Pacific Island Government for Over a Week', 18 November 2022.
8. UN, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', A/76/135, 14 July 2021 (UN GGE 2021); UN, 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', A/AC.290/2021/CRP.2, 10 March 2021. Of particular importance is the guidance on CI provided by UN GGE 2021 and the examples of sectors that should be considered critical by member states given in UN, 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'.

basis – which shows that despite the agreement on indicators, views differ on the use of the threshold.

Impact

The discussion on scale, scope and speed is indissociable from the evaluation of the impact or effects of such incidents. In addition to economic loss and scale of disruption, states noted that they will consider incidents a national security concern when they have a 'damaging and destabilising effect', as well as when there is any threat to life. In the case of the latter, one participant suggested that 'the impact of the incident matters more than the mechanism'.

For Costa Rica, the scale of economic damage extends far beyond the requested amount for the ransom. Criminals initially asked for $10–20 million but attacks against the treasury resulted in an estimated loss of $38–62 million.

As raised by Vanuatu, small island countries are even more susceptible to ransomware incidents – where the economic impacts can be comparable to those of natural disasters. Other states reiterated the importance of dealing not only with immediate unavailability of access to data but being more attentive to the medium to longer-term impacts such as the one highlighted by Vanuatu.

Motivation

Some states noted that carefully assessing and evaluating the motivations of malicious groups is fundamental to the classification of an incident as a national security threat. As highlighted by Costa Rica, the fact that the criminal group had been sending messages to the government saying that 'we are determined to overthrow the government by means of a cyber attack, we have already shown you all the strength and power'[9] was particularly illustrative of threat actor motivations when assessed in conjunction with the disruption caused and persistence of the activities conducted by the group.

In the case of Vanuatu, motivation and intention became evident because malicious actors not only harvested data but sought to use it as leverage to perpetrate other attacks. It shows that despite the criminal activities of extortion and exfiltration, these actors wanted not only to go after government services, but to exploit other sectors too.

9. Jonathan Reed, 'Costa Rica State of Emergency Declared After Ransomware Attacks', Security Intelligence, 16 November 2022, <https://securityintelligence.com/news/costa-rica-state-emergency-ransomware/>, accessed 15 August 2023.

Funding

Representatives highlighted the importance of states effectively prosecuting criminal groups. If there are government links to funding groups that are conducting ransomware-as-a-service or other malicious activities, some participants stated that this relates more to the international security realm. Representatives recognised the added value of strategies to investigate groups by 'following the money'. Further dialogue among states is required to better understand the relationship between criminal prosecution mechanisms and sanctions vis-à-vis the framework for responsible state behaviour.

Reserving the Right Not to Define the Threshold

Representatives also noted that despite the importance of distinguishing criminal, national security and international peace and security dimensions of ransomware and other emerging threats, states might wish not to publicly indicate what the threshold is – and to therefore retain the option of determining what and when an incident meets the national security concern on a case-by-case basis. Determining the threshold might also be dependent on political prioritisation (or lack thereof) and/or level of capacity to do so.

A decision to not determine the threshold provides strategic ambiguity for the state to respond to criminal groups or state-linked actors. At the same time, determining the threshold too clearly could signal permissibility – anything below the threshold would not be as strongly prosecuted.

However, as discussed during the event, wherever the threshold may lie, the discussion should centre around when and under which circumstances criminal mechanisms should be complemented by international ones. Further dialogue on responses to ransomware would help determine what kinds of incidents relate to the scope of the OEWG. States should continue to review/share case studies to understand the evaluation and the consistency of indicators used for the assessment of ransomware incidents.

Enhancing International Cyber Crisis Assistance: From Lessons Learned to Effective Coordination in Prevention and Response

In 2015, the consensus report of the UN GGE introduced a voluntary commitment from states to 'respond to appropriate requests for assistance by another state

whose critical infrastructure has been subject to malicious ICT [information and communications technology] acts' (norm 13(h)).[10] Governments have been increasingly collaborating to respond to incidents in conflict and crisis scenarios as they relate to cyber activities. Across regions, they have been devising different models and strategic partnerships to strengthen approaches that can bolster resilience, enhance capacities and sustain responses.

There are different types of assistance depending on the severity, type and context of a case. One dimension of requests for assistance, and perhaps more 'traditionally' so, is tied to capacity building projects – concentrating in areas such as the development of national Computer Emergency Response Teams (CERTs) and the establishment of early warning systems. However, the proliferation of large-scale incidents against multiple government bodies such as Costa Rica, Vanuatu, Montenegro, Moldova, Albania and other countries propelled discussions into a slightly different arena of transnational cooperation and rapid response mechanisms.

Additionally, the use of malicious ICT tools in crises and conflict zones, such as in the case of Ukraine, has resulted in yet another set of modalities for cooperative activities and models that put considerable pressure on coordination and timeliness in response activities. Each of these types of activities, while complementary to one another, presents a diverse yet rich landscape of experiences related to this norm.

With ransomware being one of the driving causes of some international assistance cases, the second part of the discussion began with contributions from Montenegro, the UK and Microsoft. They all provided initial remarks on how they have been cooperating and coordinating internationally to respond to such incidents.

Throughout the discussion, participants addressed the following questions:

- Many state and non-state actors have actively supported other states in responding to and recovering from large-scale incidents. Based on this experience, what are the main lessons learned from that cooperation (what has worked/what needs to be done better)?
- How can states better coordinate with each other and with non-governmental stakeholders when providing assistance?

10. UN GGE 2021 provides useful guidance on the implementation of norm 13(h). Some examples include: developing templates and/or sharing experiences in devising such templates; and incentivising states that identify malicious activity originating from their territory to request assistance as a way of building trust, among others.

- From the perspective of countries that received assistance, what are some of the main points that should be considered for the enhancement of future rapid response actions?
- How should these experiences inform the implementation of 'norm h' on requests for assistance?

Montenegro provided a thorough and detailed assessment of what requesting and receiving assistance looked like when it was hit by a major ransomware incident in August 2022. The incident reportedly affected 150 workstations across 10 government institutions. Overall, as highlighted during the meeting, the incident impacted CI, public services and other parts of the government, such as the prosecutor's office and revenue and customs. At the time, France, the US, the UK, Estonia and others[11] joined efforts to support Montenegro in the investigation.

Responding to and recovering from an incident of this scale extends far beyond having the technical capacities to do so. Participants noted the following priority areas.

Ensure that Domestically Government Entities are Aware of the Criticality of the Incident

Norm 13(h) on request for assistance assumes that countries are ready or aware of what kinds of support they might need. While that can be the case for some, depending on the scale and level of disruption from the incident, victim states might become overstretched in who they need to speak to. Some representatives also noted that sometimes the biggest challenge at the time of the incident is to convince other government stakeholders of the impact and criticality of an incident. In some cases, politicians remained agnostic about large-scale ransomware incidents until they started being reported and/or they discussed with national experts.

Other representatives noted that knowledge of the incident is also crucial if a malicious activity is emanating from the territory of a particular state. This is particularly relevant for demonstrating due diligence. As noted, and as further elaborated in UN GGE 2021, if the state whose territory might have been identified as the origin of malicious activity offers to provide assistance (or even requests

11. Misha Savic, 'Ransomware Attack Sends Montenegro Reaching out to NATO Partners', *Bloomberg*, 1 September 2022; Jonathan Greig, 'Montenegro Struggles to Recover from Cyberattack that Officials Blame on Russia', *The Record*, 29 August 2022, <https://therecord.media/montenegro-struggles-to-recover-from-cyberattack-that-officials-blame-on-russia>, accessed 15 August 2023.

to receive assistance[12]), such support can 'help minimise damage, avoid misperceptions, reduce the risk of escalation and help restore trust'.

Strengthen Coordination Among and Within States Providing and/or Seeking to Provide Support to a Victim State

Some participants noted that lack of coordination among donor countries can often lead to a duplication of assistance and different expectations depending upon the donor and recipient. This shows that even if the offer of support is abundant, a lack of coordination can become an extra burden for victim countries. One of the participants noted that, at a certain stage, 15 countries were providing support to Pacific Island countries on basic steps to set up and run their CERTs. While important, the offer is indicative of multiple funding channels and highlights the need for more joint efforts in capacity building to avoid duplication.[13]

The designation of a national coordination point from the victim country is equally important to facilitate deployment of crisis response support. This could be the national CERT or other nationally relevant designated entities. As the experiences shared in the room highlighted, the victim country is often faced with an increasing pressure of having to effectively respond both to the incident and to external requests. The national coordination point should be able to be 'in the know' enough to coordinate with other government agencies on how to best direct external support for internal needs – but it does not necessarily need to be the most technical actor.

The UK proposed four points that should be considered by states in providing assistance:

1. Whenever possible, avoid waiting for the crisis. Investments in resilience may need to come upfront but in the longer run they are more cost effective than remediation.
2. Devise models internally and internationally that can respond in an agile and timely manner. As one representative noted, states might seek to close memorandum of understandings with other strategic partners and gradually build their bilateral cooperation channels to have both the administrative and relational components in place to respond to any cyber crises.
3. Horizon scanning can help states better understand their own national/regional threat landscape.

12. This is not explicitly included in UN GGE 2021.
13. UN GGE 2021 mentions the development of common templates for requests for assistance at the bilateral, multilateral and regional levels as a practical measure to support the implementation of norm 13(h).

4. On capacity building and the implementation of norm 13(h), donor countries need to better coordinate given the finite pool of resources. Furthermore, the establishment of embassy networks and cyber attachés can often significantly support cyber capacity building. However, it is crucial that the private sector is involved in assistance provision.

Develop Capacity for Proactive Monitoring and Response

In Montenegro's case, the 2022 ransomware incident led to the creation of multiple policies and bodies within the government, such as the Agency for Cybersecurity, and the publication of the 2022–2026 iteration of its national cyber security strategy[14] focusing on capacity building and raising awareness among the government and population. Costa Rica and Vanuatu have had similar domestic shifts that have enhanced the visibility and understanding of how cyber incidents relate to national security. Other developing economies also shared their own experiences in establishing ICT-focused agencies – especially small island countries that are embedding cyber security within these broader initiatives.

Other representatives raised the point that awareness of malicious ICT activities – be they ransomware or other attack types causing critical disruptions to a state – is primarily dependent on having the proper capacity to identify and respond. As noted, 'capacity building is not just about awareness of an incident but providing the infrastructure and capability to respond' in the medium to long term.

This latter point was equally highlighted by several representatives. Many participants suggested that capacity building efforts often concentrate on training activities and exercises when certain countries are in need of IT equipment. Training, albeit important, is only one part of the solution. Having access to technology and the proper setup is equally crucial for countries to effectively implement and allocate the human resources that have been part of trainings and other capacity building efforts.

Conclusion and Reflections for Future Dialogues

The inclusion of ransomware in the 2023 Annual Progress Report shows that states see this particular cyber threat as a shared concern. While far from being the only or the single most important threat, ransomware stands out because

14. EU Cyber Direct, 'Montenegro', <https://eucyberdirect.eu/atlas/country/montenegro>, accessed 1 September 2023.

it has greatly affected developed and developing countries alike. As such, it can bring a diverse array of countries to the table for an informative and constructive dialogue on responsible state behaviour.[15]

Additionally, representatives suggested that collaboration and exchanges on defining the impact of incidents as they relate to the economic, social and cultural dynamics of a country could help the identification of common approaches to impact measurement and interpretation. As the dialogue showed, ransomware can have disproportionate effects in developing economies. This is particularly the case with economic losses resulting from incidents. A regional or development-sensitive approach to impacts and emerging threats could positively contribute to further the understanding of how responsible state behaviour and implementation of the acquis relate to development and capacity builidng strategies.

On cooperation during crises, it became clear that having the capacity to respond to a cyber crisis is not just a question of technology, infrastructure or human resources, but of having the appropriate mechanisms in place – and being capable of mobilising them in a timely manner. While procurement was often referred to as being time-consuming and slow, representatives suggested that it would be beneficial to have a network or an effort to map rapid-response teams/deployments and other capabilities that could be used in time of crises. Furthermore, cooperative crisis response strategies can be further enhanced when they are the result of a layered process where existing bilateral, multistakeholder and regional trust building efforts help speed up and enhance timely responses.

As the dialogue highlighted, a thorough discussion on ransomware can help untangle some important challenges facing the OEWG and broader international cyber cooperation – that is, what distinguishes a criminal approach from an international security approach; how crisis response and other international assistance experience can help inform future or existing norms; what kinds of capacities are required/expected in conducting response activities.

Having a facilitated platform for exchange where stakeholders can participate and bring practical inputs is particularly useful to complement governments' experiences in handling large-scale incidents. The OEWG, PoA and other multistakeholder spaces can and should support that continuation at the international level. An emerging model for non-political information exchange

15. The recommendations provided reflect points raised during the dialogue and do not necessarily reflect Estonia's, Costa Rica's or Vanuatu's official views on the matter.

can help build trust, enhance transparency over responsible state behaviour, and serve as an example for other cyber-related international security threats.[16]

Louise Marie Hurel is a Research Fellow in the Cyber team at RUSI.

16. RUSI-specific recommendation: The 2023 APR mentioned the need for further discussion on threats and potentially an intersessional on the topic. During the event, states recognised the need for more discussion on ransomware and other emerging threats. States could consider how/if either the OEWG or the PoA could foster a post-mortem non-political assessment of incidents, where member states can voluntarily propose a meeting and share their lessons from responding and recovering, as this side event did – in conjunction with other stakeholders. This could serve as a model for enhancing guidance on norms implementation as they respond and relate to an evolving threat landscape. It could also include other threats, such as the use of generative AI – a topic of the latest Arria formula meeting of the UN Security Council in July 2023.