kaspersky

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Submission on 'Responsible state behaviour in cyberspace in the context of international security at the United Nations"

As a global cybersecurity company, we are grateful for the opportunity to share our suggestions and recommendations on best practice implementation of the cyber norms set out in the 2015 GGE report.

1. **What existing and emerging threats should inform Australia's approach to discussions on the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) in the OEWG and GGE?**

   Among the threats risking international peace and security, we would like to highlight first that the international community remains fragmented, while cybercriminals – ranging from state-backed cyberespionage groups to common thieves – only benefit: they can target anyone, anywhere, from anywhere, to spread fear, uncertainty and doubt throughout cyberspace. The growing mistrust among nation states and militarization of cyberspace is aggravated by the following factors:

   1.1. First, both conceptually and methodologically, ***cyberspace is transforming into a new field for interstate military conflict***[1] – in addition to the traditional air, land and sea-based military fields. We at Kaspersky[2] investigate and monitor more than 300 Advanced Persistent Threat (APT) operations that refer to the groups – often state sponsored or well-funded in other ways – that are responsible for launching such precision attacks.

   1.2. Second, because of the ***dual-use nature of internet infrastructure***, it could be used as a weapon in cyber-conflicts and thus lead to spill-over of military actions into the civilian sphere with unintended damage and effects.

   1.3. Third, ***lack of communication and dialogue among state and non-state actors*** increases the potential for escalation of conflicts in cyberspace, while malicious non-state actors become ***more diverse with differing motives*** making the cyberspace more chaotic and less predictable.

   1.4. Finally, the use of false flags has become an important element in the playbook of several APT groups, and we anticipate a ***next level of false flag attacks*** when threat actors will seek not only to avoid attribution but to actively lay the blame on someone else. For instance, this could include the usage of established backdoors by other unrelated APT actors, the theft and re-use of code (the recently published case of Turla reusing code from an unknown Iranian group[3] outlined by the UK NCSC and NSA comes to mind) or deliberately leaking source code so that other groups adopt it and muddy the waters further. In one notable case – the Olympic Destroyer attack[4] – the Hades APT group sought to go further than just clouding waters of attribution by forging elements of the attack to make it look like the work of a different threat actor.

   At the same time, analyzing the nature of attacks and APT operations, we observe the following security risks have the potential to impact the security landscape dramatically:

   2.1. **Increasing sophistication of attack methods and growing risk of supply chain attacks.** Use of supply chains continues to be one of the most difficult delivery methods to address, and it is likely that attackers will continue to expand this method through manipulated software containers, for example, and abuse of packages and libraries. At the same time, the new isolation methods implemented for popular software traditionally targeted in spear-phishing campaigns might have a significant impact on malware delivery methods, forcing less sophisticated actors to change the way they spread malware. It also seems likely that attackers will exfiltrate data with non-conventional methods, such as using signaling data or Wi-Fi/4G – especially when using physical

[1] https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[2] https://www.kaspersky.com/blog/apt/2050/
[3] https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims
[4] https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/

implants (something we also believe is probably being overlooked). In a similar vein, we believe more attackers will use DoH (DNS over HTTPS) in the future to conceal their activities and make discovery more difficult. Finally, it is possible that during the coming months we will start discovering more UEFI malware and infections as our ability to see such systems is slowly improving.

2.2. **Destructive and targeted ransomware attacks.** Though in the last two years we have seen a decline[5] in numbers of all-purpose widespread ransomware attacks, ransomware still remains a highly destructive attack and most effective tool for extracting financial profit from victims. Cybercriminals have become more strategic[6] in their use of this type of malware – focusing on organizations that are likely to make substantial payments in order to recover their data. An additional twist might be that, instead of making files unrecoverable, threat actors will threaten to publish data that they have stolen from the victim company.

2.3. **More critical infrastructure attacks.** Determined threat actors have, for some time, been extending their toolsets beyond Windows, and even beyond PC systems: VPNFilter[7] and Slingshot[8] operations, for example, targeted networking hardware. The benefit to an attacker, of course, is that once they have compromised such devices, it gives them multiple options for attack development: they could opt for a massive botnet-style compromise and use that network in the future for different goals, or they might approach selected targets for more clandestine attacks. In addition, in recent years we have seen a number of high-profile attacks on critical infrastructure facilities and these have typically been aligned to wider geo-political objectives. While most infections[9] in industrial facilities continue to be coming from 'mainstream' malware, this fact itself highlights just how vulnerable these facilities can be. While targeted attacks on critical infrastructure facilities are unlikely ever to become a mainstream criminal activity, we do expect to see their number grow in the future. Geo-political conflicts are now played out in a world where physical and cyber are increasingly converging; and, as we have observed before, such attacks offer governments a form of retaliation that lies between diplomacy and war.

2.4. **Internet of Things (IoT) and embedded systems in smart cities and smart industries as a new attractive vector for cyberattacks.** Poorly secured consumer IoT devices as well as industrial IoT systems embedded in the smart cities and smart industry projects are an increasingly attractive target for malicious actors. In H1 2019, we detected[10] more than 100 million attacks on smart devices, and based on data analysis. While these attacks are usually not very sophisticated, they are hard to detect as both home users and industries might not even notice their IoT devices being exploited. On the enterprise side, the vast majority of IoT-based attacks use the botnet-powered distributed denial of service (DDos) technique to exploit numerous IoT devices that control critical infrastructure or some important societal functions.

2.5. **Attacks with the use of machine learning.** We expect the growing interest of threat actors in adopting machine learning to create highly sophisticated attack code that would be able to evolve through learning more about attack environments; they would also allow threat actors to maintain a long-term presence in their target environments as well as to compromise systems with a minimal chance of detection.

2. Are there any specific areas of the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) that, from your

---

[5] https://securelist.com/ransomware-and-malicious-crypto-miners-in-2016-2018/86238/
[6] https://securelist.com/sodin-ransomware/91473/
[7] https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/
[8] https://securelist.com/apt-slingshot/84312/
[9] https://www.kaspersky.com/about/press-releases/2019_mining-spying-self-replicating-energy-sector-under-cyberthreat-pressure
[10] https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

perspective, should be further developed in the OEWG/GGE? If so, how would you like to see these areas addressed in any OEWG and/or GGE report(s)?

For achieving the stability and security of cyberspace through an effectively working framework for Responsible State Behaviour, it is crucial to address the following challenges and gaps:

1.1. **Clear division of responsibilities and functions between the OEWG and GGE for greater synergy**. We share the concern[11] that two processes might arrive at contradictory outcomes or fail to achieve a result at all. Public OEWG consultations held in September 2019 demonstrated that states have distinct and sometimes incompatible views on the division of roles and labour between the OEWG and GGE. Therefore, taking into account the limited time of the mandates for two processes, it is essential to reach a consensus over division of topics, transparent channels for information exchange as well as ensuring communication and cooperation at the level of groups' Chairs and Secretariats.

1.2. **Further consultative work on harmonization of application of international law in cyberspace, namely in regard to the principle of the sovereignty**. Publicly available documents where some states[12] have expressed their position on the application of international law in cyberspace demonstrate states' divergence in how and to what extent the principle of the sovereignty applies. For instance, the UK[13] has taken the position that respect for sovereignty is not a primary rule in cyberspace and, in particular, a remote cyber operation by one country in another's cyber infrastructure does not violate the latter's sovereignty. France, on the contrary, fully recognizes[14] the principle of state sovereignty in cyberspace and does highlight that a hostile cyber operation against French cyber infrastructure or one causing 'effects' on French territory violates French sovereignty. As a private global company protecting clients in various parts of the world, we see a greater risk of unintended damage and effects in cyberspace affecting both companies and users as a result of different views of states on fundamental principles of international law. Therefore, we believe that clear 'rules of the game' may prevent escalation as it becomes more understandable to the participants. These rules may lower the chance that the states involved in a cyber exchange will misinterpret the actions of their opponents.

1.3. **Further consultative work on harmonization of definitions.** Consensus over definitions, terms and concepts would increase clarity in states' actions and policy discussions, as well as contribute to mutual understanding among actors. As an example, the Global Commission on the Stability of Cyberspace (GCSC) worked on the common definition of Cyber Stability and sought feedback on the proposed draft. Not only did we take part and share our comments[15], but we also highly welcomed such efforts to obtain views ensuring a transparent, open and multistakeholder approach.

1.4. **Open collaborative work on the widespread use of technical standards that ensure cyberspace is resilient.** Following the conclusions[16] in the Final Report by the GCSC, we firmly support further development, open promulgation and widespread use of technical standards. Cooperative work on the technical standards as a separate element of the framework for Responsible State Behaviour in Cyberspace would allow to overcome the increasing fragmentation and inconsistency in global cybersecurity efforts, including regulatory and legal practices.

1.5. **Further consultative work on the operationalization of norms with a wide representation of the private sector, academia and other stakeholders.** We strongly believe a multistakeholder

---

[11] https://www.unidir.org/sites/default/files/conferences/pdfs/cyber-stability-conference-2019-summary-report-eng-0-849.pdf
[12] These states are Australia, Canada, Estonia, France, the Netherlands, the UK.
[13] https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century
[14] https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf
[15] Kaspersky has been named as one of the contributors to the Final Report https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019-1.pdf
[16] https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019-1.pdf

dialogue and efforts to make GGE norms[17] operational would bring enormous value for greater cyber stability and peace. Such working discussions have to include both state and non-state actors to develop transparent mechanisms that enable their responsible behavior in cyberspace. As an example, we would like to mention the successful launch of a series of such dialogues on operationalizing cyber norms by UNIDIR. In January 2020, Kaspersky took part in the first round of such talks dedicated to the existing approach to Responsible Vulnerabilities Disclosure[18].

3. **As stated above, a key Australian objective is for the OEWG and/or GGE to provide practical guidance on observation and implementation of the agreed norms of responsible state behaviour, set out in the 2015 GGE report (found here). What do you consider to be best practice observation and implementation of these norms? We welcome your input of concrete examples/suggestions of best practice implementation of one, some, or all of the norms (see Annex A), which could be considered for incorporation into any report of the OEWG and/or GGE.**

Following the table in the Annex A, we share our suggestions on best practice implementation to some norms below:

Norm	**Examples of best practice implementation of the Norm**
(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.	We believe that further development of clear industry standards, technical requirements and security measures applied to ICT products and services will help build cyber resilience globally. Such standards and best practices have to be industry-led, consensus driven, interoperable and global to ensure they are applied consistently and universally. A good example of such efforts is the Cybersecurity Act of the European Union, which prescribes the creation of the European Cybersecurity Certification Framework[19] through a multistakeholder approach (namely, through a creation of Ad-Hoc Working Groups and the Stakeholder Cybersecurity Certification Group). An additional example is the publication of draft guidelines on data protection 'by design' and 'by default' by the European Data Protection Board for a public consultation[20]. This illustrates how the concept and its technical and organizational measures have to be developed and applied according to industry's best practices and experience. Kaspersky has also shared its recommendations[21].
(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences; States should not knowingly allow	To overcome the lack of attribution or misattribution which can lead to escalation of tensions between states, it is necessary to develop transparent and trusted platforms for exchange of threat information between private actors and government agencies, including CERTs.

[17] As adopted by the 2015 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 https://undocs.org/A/70/174
[18] https://unidir.org/events/operationalizing-cyber-norms-multi-stakeholder-approaches-responsible-vulnerabilities
[19] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[20] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en
[21] https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/kasperskys_submission_on_the_guidelines_on_article_25_data_protection_by_design_and_by_default.pdf

their territory to be used for internationally wrongful acts using ICTs.	As an example of the private sector's approach, Kaspersky developed its Threat Intelligence Portal[22] to provide access to technical descriptions of the very latest threats during an ongoing investigation; insight into non-public investigations; detailed supporting technical data and access to our YARA rules; continuous campaign monitoring; and access to actionable intelligence during an investigation (information on campaign distribution, IOCs, C&C infrastructure). As a support to cyber capacity building in the fight against cybercrime, we provide freemuim access to the Portal within our free package for Law Enforcement Agencies[23]. Another example of public-private cooperation for information sharing is our contribution agreement with INTERPOL[24], signed in July 2019 – we pledged to provide human resources support, training, and threat intelligence data on the latest cybercriminal activities to INTERPOL, strengthening the organization's cyberthreat hunting capabilities.
(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.	As a best practice implementation of this norm, we would like to highlight the EU Security of Networks and Information Systems (NIS) Directive[25], which has produced sector cybersecurity guidance and developed a framework to support the assessment of cyber-resilience of regulated organizations (i.e., operators of critical infrastructure and digital service providers). In 2018, the UK also implemented the NIS Directive[26] after a public consultation to collect proposals from private actors on introducing the cross-sector Critical National Infrastructure (CNI) regulation. In particular, we highly welcome several aspects of the NIS Directive such as establishing cooperation of CERTs, rules, procedures and thresholds for incident response as well as transparent reporting requirements.
(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.	Supply chain attacks remain the most destructive and difficult to prevent. Therefore, for the implementation of this norm is crucial to develop frameworks for technical and institutional evaluation of the trustworthiness of supply chain vendors. From the vendor side, it is important to ensure the integrity of the supply chain through the publicly communicated policies and practices. Our Global Transparency Initiative (GTI)[27] as a set of practical measures to increase transparency and accountability in cybersecurity could be a guiding example for the private sector. Practically speaking, the GTI includes framework to build trust and confidence of users in cybersecurity: • **Data Care**: relocation of data processing and data storage to Switzerland – a state with long famous neutrality and strict data protection regulation;

[22] https://opentip.kaspersky.com/
[23] https://media.kaspersky.com/en/enterprise-security/supporting-law-enforcement-agencies.pdf
[24] https://www.kaspersky.com/about/press-releases/2019_kaspersky-extends-cooperation-with-interpol-in-joint-fight-against-cybercrime
[25] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[26] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[27] https://www.kaspersky.com/transparency-center

	• **Dedicated Transparency Centers**[28] for accessing Kaspersky's source code, software updates and threat detection rules, along with other activities, for external review. There we also provide access to review types of information which, in general, Kaspersky products send to our cloud-based Kaspersky Security Network (KSN); and rebuild the source code to make sure it corresponds to publicly available modules. Our Transparency Centers are located in Zurich and Madrid and will soon be launched in Kuala Lumpur and São Paulo; • **Secure and reliable engineering practices** confirmed through third-party independent assessments, including the SOC 2 audit by a 'Big Four' accountancy firm[29] and ISO 27001 certification (to be publicly announced in February 2020); • **Vulnerability Management Program**: responsible cooperation with security researchers and a Bug Bounty Program with awards of up to $100k for the most critical flaws found in Kaspersky's systems. For ensuring the security of supply chains in the IoT, we also welcome the following initiatives that Kaspersky was invited to participate: 1) the UK Consumer IoT Security Code of Practice[30] - which was the basis of the ETSI TS 103 645 standard; and 2) ENISA's annual studies for the Good Practices for Security of IoT – Secure Software Development Lifecycle[31]. These examples illustrate cooperative work to address existing gaps in software development, and we believe that this format with industry's engagement in producing guidelines and best practices for addressing supply chain risks has to be applied further.
(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.	We highly welcome the developing efforts of several states to establish transparent policies for responsible vulnerability disclosure (for instance, policies that are set up by Australia[32], the Netherlands[33]), and a bug bounty program running together with a third party (for instance the UK NCSC Bug Bounty Program[34] at HackerOne or the Bug Bounty Program run by the Government Technology Agency (GovTech) and Cyber Security Agency (CSA) of Singapore[35]).

[28] https://www.kaspersky.com/transparency-center-offices
[29] https://www.kaspersky.com/about/compliance-soc2
[30] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
[31] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
[32] https://www.cyber.gov.au/tags/security-vulnerability
[33] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[34] https://hackerone.com/ncsc_uk
[35] https://www.csa.gov.sg/news/press-releases/second-government-bug-bounty-programme-expanded-to-cover-more-systems-and-digital-services

	We at Kaspersky run our program for transparent coordinated vulnerability disclosure called Vulnerability Report[36] as well as our Bug Bounty Program together with HackerOne mentioned above. In 2018, we also took part in the study[37] by the Centre for Policy Studies (CEPS) under the chairmanship of Ms. Schaake – a former member of the European Parliament. Within a working group with other companies we discussed challenges to software CVD in Europe and as an outcome prepared practical recommendations to address existing challenges. In addition, at the UNIDIR Workshop dedicated to operationalizing cyber norms (mentioned above), it was widely discussed and agreed that risks of legal proceedings and lack of transparent policies with trusted communication channels are often key challenges to the greater security of products and applications available on the market. To address that, we at Kaspersky joined the Dislose.io[38] project to offer a safe harbor for security researchers – we pledged not to initiate legal proceedings against those who look to research our products and find vulnerabilities in there.

4. **The mandate of the GGE invites members to annex to the GGE report "national contributions…on the subject of how international law applies to the use of information and communications technologies by States". Through the International Cyber Engagement Strategy, Australia has published its positions on the application of international law to cyberspace in 2017 and 2019 (found here). Are there any relevant areas of international law that that, from your perspective, should be addressed in any Australian contribution to the international law annex to the GGE report? If so, how would you like to see these areas addressed?**

   Following the position on the application of international law to cyberspace[39], we noticed that the Australian Government has not explicitly commented on issues relating to attribution of cyber operations; definition of interference/intervention; and its position to the application of the principle of sovereignty in cyberspace. An explicit opinion of the Australian Government would provide additional clarity on how those questions are addressed compared to the positions of other countries.

5. **Another key Australian objective is for any report of the OEWG and/or GGE to make recommendations on better coordinating global cyber capacity building. We welcome suggestions on how coordination of global cyber capacity building might be improved, as well as how you would like this to be addressed in any OEWG and/or GGE report(s).**

   We believe that further global cyber capacity building might be improved through:

   1.1. **Open sharing and exchange of national cybersecurity strategies, as well as best practices on designing policies and drafting legislation among states and with the private sector**. While their elements and principles are usually similar, the level of their implementation varies. The clarity of objectives (i.e., economic and social development, fight against the cybercrime,

[36] https://support.kaspersky.com/general/vulnerability
[37] https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/
[38] https://www.kaspersky.com/blog/kaspersky-joins-disclose-io/27588/
[39] https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html

etc.) and the mandate for each organization are critical to apportioning who should do what. As an example, we highly welcomed the public consultation launched[40] by India's National Security Council on National Cyber Security Strategy 2020, or by Australia on the national 2020 Cyber Security Strategy[41]. These examples illustrate greater transparency and dialogue with the private sector, and we believe would be more effective.

1.2. **Creating a cybersecurity competence network for greater coordination between research centers, SMEs, and cybersecurity companies.** For greater synergies, we believe it would be great to explore opportunities for establishing a cybersecurity competence network for research and development programs in cybersecurity where governments would have an opportunity to clearly define calls for necessary technologies, tools and projects needed. Research centers, universities, SMEs, companies, industry and others – all would have the opportunity, through a transparent selection process and eligibility criteria, to take part in collaborative projects and get government funding. Such an approach would make market needs and national cybersecurity better aligned.

1.3. **Organizing large-scale national awareness cybersecurity campaigns for greater cyber-hygiene.** We believe that nationwide campaigns would be a good example to engage numerous actors of different scale and size in developing a holistic understanding of cybersecurity and cybercrime, with basic steps such actors should take to protect themselves. A successful example of such actions is the European Cybersecurity Month[42], which in 2018 led to a total of 532 activities across 33 countries in Europe on a wide range of topics.

1.4. **Contributing to public-private partnerships (PPPs) in cybersecurity**. Voluntary PPPs help enhance public-private operational collaboration to address cybersecurity threats. A special focus could be made on PPPs for assisting SMEs and citizens to cope with challenges which the digital transformation creates. As an example, we successfully cooperate within the NoMoreRansom project[43] – established in 2016 together with Europol, the Dutch police and McAfee. This is a non-commercial public-private project for helping victims of ransomware to decrypt their data. This project has been named the gold standard among PPPs and attracted 150+ project partners representing public and private organizations from around the globe.

6. What role should the business/government/NGO/academic community play in promoting a peaceful and stable online environment? How would you like to see this addressed in any OEWG and/or GGE report(s), or any Australian contribution to the annex to the GGE report?

We believe that all actors mentioned in the question could work together to address the gaps in the following fields:

- further development of security requirements and technical standards for cybersecurity products and services;
- promoting responsible vulnerability disclosure and establishing country-specific transparent policies and guidelines;
- creating open platforms for public-private cooperation in cybersecurity and for threat information sharing.

These directions could be explicitly addressed in both the OEWG and GGE reports as areas for multistakeholder action and confidence-building.

---

[40] https://ncss2020.nic.in/
[41] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020
[42] https://cybersecuritymonth.eu/
[43] https://www.nomoreransom.org/

About Kaspersky
Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Contact
For more information, or to discuss the contents of this submission in more detail, please contact Anastasiya Kazakova, Public Affairs Manager (+7 968 648 60 05 | Anastasiya.Kazakova@kaspersky.com).