CHAIR'S REPORT OF THE MEETING OF THE G7 ISE-SHIMA CYBER GROUP

(undated; endorsed by the G7 Foreign Ministers' Communiqué from 23 April 2018)

1. All G7 partners reiterated their shared vision of an accessible, open, interoperable, reliable and secure cyberspace the benefits of which can be enjoyed by all. Recognizing the enormous economic, political and social benefits that can be derived from cyberspace, partners emphasized the need for collaborative and inclusive approaches that benefit from the participation of all stakeholders, including the private sector, civil society, academia and governments. Bearing in mind that opportunities and impacts—positive and negative—are experienced differently by different groups, including by women and children, LGBT groups, and marginalized communities, and noting the digital divides between and within countries, the need for positive action to address these inequalities was emphasized.
2. The group noted that threats to the accessible, open, interoperable, reliable and secure cyberspace are on the rise. Against this background, G7 partners emphasised the importance of developing policies to promote digital security and to ensure trust and stability in cyberspace, taking into account the responsibility of all actors, including those from the government and private sector, to contribute to this effort.
3. States, their proxies and non-state actors are undertaking malicious cyber activity intended to undermine democratic process and institutions, as well to threaten critical infrastructure and the economic well-being of liberal democracies around the world. Particular attention was drawn to recent national statements by some G7 and other partners ascribing responsibility to Russian actors for the reckless and uncontrolled NotPetya cyber attack, which started in Ukraine and spread globally, causing billions of dollars in damage to companies around the world. Similarly, the group reviewed the national statements linking North Korea to the WannaCry ransomware attack, which affected the UK National Health System and destroyed information on millions of computers around the world.
4. The rising sophistication and cost of cybercrime was also discussed, including the increasing role of transnational organized crime and the links with state actors. The group also considered the possible use of cyber-enabled theft and of cryptocurrencies to raise and transfer funds outside the reach of multilateral sanctions regimes, including by North Korea, or for the purpose of terrorist financing and money laundering. The group reiterated their shared commitment to the Budapest Convention on Cybercrime. They highlighted its continued relevance, evidenced by the diverse and growing group of states across six continents that have joined or are considering joining the Convention, and the negotiations now in progress to establish a new protocol to the Convention. The group recognized the importance of the work on cybercrime under the auspices of the UN Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, and their shared focus on capacity-building and further international cooperation in this regard. The use of the Internet for terrorist purposes, including recruitment, training, coordination, incitement to imminent violence, and fundraising, continues to be a major concern and a focus of coordinated G7 action. Efforts in the G7 Roma-Lyon Group and the G7 security ministers meetings on countering violent extremist and terrorist use of the Internet were noted.
5. They noted with concern the decline of Internet freedom, including the growing use of Internet shutdowns, restrictions on the use of virtual private networks, restrictions on access to information and freedom of expression, violation of the right to privacy and cyber attacks on journalists, human rights workers, democracy activists and civil society groups. They emphasized that the same rights that people have offline must also be protected online and

reaffirmed the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties.

6. Partners recognized the important role the G7 plays in addressing these growing threats. As liberal democracies, it was recognized that our approaches must be based upon our shared commitment to international law, democratic values, institutions and processes, human rights, inclusivity, openness, transparency and the rule of law. The resiliency of our societies comes as a result of these qualities; our responses must therefore reinforce them. An important dimension of these responses will be applying democratic governance frameworks created for an analog world to a rapidly evolving digital age in which emerging technologies such as artificial intelligence, the "Internet of Things", robotics and other technologies continue to both empower people and grow the economy, and impact political, social, economic and cultural relationships within and among states.
7. Partners expressed regret that the most recent United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE) was unable to adopt a consensus report in 2017 when some countries' experts walked back from previous reports' statements on the applicability of international law to states' activities in cyber space; an outcome which should concern all those committed to security and stability in cyber space. They emphasized that despite this outcome, the recommendations contained in the 2010, 2013 and 2015 UN GGE reports remain valid. They decided to continue to support efforts, at the UN and elsewhere, to promote affirmation of the applicability of existing international law to states' cyber activities – including the UN Charter and customary international law, and notably international humanitarian law and international human rights law as well as the promotion and implementation of certain voluntary, non-binding peace-time norms of responsible state behaviour.
8. The group recalled and reiterated the statements and commitments made in the G7 Lucca Declaration On Responsible State Behavior In Cyberspace, including in particular: the call for increased international cooperation on cyber security; the commitment to conflict prevention and the peaceful settlement of disputes; the applicability of existing international law and the promotion of voluntary, non-binding norms of responsible state behavior in cyberspace during peacetime; and the call upon all States to be guided in their use of information and communications technologies (ICTs) by the cumulative reports of the UN GGEs.
9. They noted with pleasure the advancement of these issues in other settings, including the establishment for the first time of cyber security confidence-building measures in the Organization of American States, the establishment of the Inter-Sessional Meeting on ICTs Security within the ASEAN Regional Forum, the prospect of the adoption of a Cyber Declaration by the Commonwealth Heads of Government, the development of a Joint EU Diplomatic Response Framework to Malicious Cyber Activities and EU Cybersecurity Package 2017, and the adoption of a Cyber Defence Pledge, framed in the context of respect for international law and strategic stability, by NATO. The Group lauded the efforts by the Hungarian Chair of the CBM Working Group and the Italian Chair in Office to advance cyber issues within the Organization for Security and Cooperation in Europe and expressed hope that all OSCE participating states would adopt a more constructive approach in support of these efforts.
10. In light of the growing cyber threat to liberal democracies, G7 partners committed to continuing the development of mechanisms for coordinated responses to malicious cyber acts. We plan to work together with other governments and stakeholders that share our commitment to democracy, human rights, and the rules-based international order, including international law and non-binding norms of state of behaviour, to develop mechanisms to

signal clearly our understanding of what constitutes unacceptable behaviour in cyberspace and to join one another in imposing consequences on those undertaking such behaviour.

11. Noting the obstacles to the investigation and prosecution resulting from cross-border evidence issues, the group expressed their support for the continued multi-stakeholder work under the auspices of the Internet and Jurisdiction Policy Network, including most recently the Ottawa Road Map that came out of the 2nd Global Conference on Internet and Jurisdiction held in Ottawa in February 2018.
12. The group concurred on the need to consider and counter technology facilitated violence against women and children and marginalized communities. The need for a better coordination on efforts to counter this type of violence among states was raised, as well as the need to apply existing legal levers to prosecute perpetrators to the best extent possible and to work with intermediaries, including social media platforms, in finding effective solutions.