

1
2 **FORUM:** **First Committee**

3
4 **QUESTION OF:** **Digital Warfare**

5
6 **CO-SUBMITTED BY:** **Canada, South Africa, Iran, United Kingdom, Germany, Bahrain**

7
8 The First Committee,

9
10 *Alarmed* by the past and continuous increase and severity in digital warfare across borders,

11
12 *Taking into account* that networks and communication systems have become a key factor in
13 economic and social development, and that their availability and integrity is crucial to essential
14 infrastructures, as well as to public and private services and the economy as a whole,

15
16 *Expecting* that the future will bring even greater interconnectivity to the world's computer networks,
17 which will result in higher vulnerability to security systems,

18
19 *Observing* the priority some States place upon the investigation of abuse of these means of
20 communication,

21
22 *Noting* that insufficient international efforts have been made to research and counter these potential
23 threats to global peace and security,

24
25 *Realizing* the shortage of international legislation, and the calls for supporting legislation to closely
26 monitor groups that commit acts of information warfare,

27
28 *Conscious* of the need for individuals, businesses, administrations, and other organizations to
29 protect their information, data and communication systems by deploying effective security
30 technologies where appropriate,

31
32 *Deeply convinced* that this problem can only be solved by a broad international coöperator,

33
34 1. *Calls upon* all UN member States to take measures within their national boundaries on this
35 matter;

36
37 2. *Requests* the Secretary-General and Member States to install a multinational task force on
38 digital warfare responsible with the primary tasks:

- 39
40 a) To research on the subject of digital warfare, and to inform the General Assembly of
41 developments in digital warfare by :
- 42
43 i) Collecting semi-annual reports from UN member States on intelligence assessments;
44 ii) Gathering information from non-state parties;
45 iii) Publishing comprehensive semi-annual reports on this collected data;
- 46
47
48 b) To install an advisory task force which operates as emergency response team, and
49 acts as an international early warning system, under the supervision of the Security
50 Council;

- 51
52 3. *Calls* for strong cooperation to develop legislation on digital warfare under present
53 international law, to react when a government perceives that there exists a significant and immediate
54 threat to international security;
55
56 4. *Urges* all States to provide globally standardised principles on authentication and security by
57 removing the remaining controls on the free use of, and trade in, encryption products for the
58 protection of privacy;
59
60 5. *Summons* an international conference in order to draft a treaty on the ban of digital warfare
61 as a means in international conflicts;
62
63 6. *Invites* all corporations, organisations and governments to share their knowledge on
64 advancements in methods to improve the protection of computer networks;
65
66 7. *Expresses* its hope that all member States will cooperate on this matter.