Statement regarding CIA Hacking tools

The Just Net Coalition[1] (JNC) was formed at a civil society meeting in New Delhi in February 2014. It comprises several dozen organisations and individuals from different regions globally concerned with internet governance, human rights and social justice, and the relationship between them.

In March 2017, Wikileaks published information on use by the US Central Intelligence Agency (CIA) of various hacking tools and malware, see:

https://wikileaks.org/ciav7p1/

According to that information, the tools in question include malware that can be used to infect various Internet of Things (IoT) devices, including home television sets (TVs), and can be used to monitor conversations near the TV even if the user thinks that the TV has been turned off. Further, similar capabilities can be used to infect smartphones and turn them into monitoring devices, even when the user thinks that they have been turned off.

Worse, according to the information published by Wikileaks, the CIA has lost control of its arsenal of hacking tools, which are now available to entities other than the CIA, including presumably cyber-criminals.

Even worse, the tools are designed to conceal who is using them, so attacks using these tools cannot be traced back to the source of the attack. Instead, the source appears to be some unrelated third party, who then gets blamed for the attack.

As we stated in our Delhi Declaration[2], "The Internet must be used only for peaceful purposes and this must be recognised by states in a binding and enforceable instrument."

The revelations concerning the CIA, and its loss of control of hacking tools, underscore the importance of implementing that principle. It is increasingly apparent that the security of IoT devices is inadequate[3] and that that could have catastrophic consequences[4]. Further, unlike physical weapons, cyber-weapons can be replicated at essentially no cost, so their production and stockpiling presents dangers that are even greater than the production and stockpiling of physical weapons.

Consequently, we call on all sectors of society, including governments, to adhere to the cited principle of our Delhi Declaration. In particular, we call on all states to agree, in an instrument binding under international law:

---

1 http://justnetcoalition.org

2 http://www.justnetcoalition.org/delhi-declaration

3 See for example p. 107 of the Global Internet Report 2016 of the Internt Society, available at: https://www.internetsociety.org/globalinternetreport/2016/

4 See for example: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/01072016/Documents/S1P3_Corinna_Schmitt_v3.pdf ; see also the "weaponization of everything", p. 2 of the report of the Global Commission on Internet Governance, available at: http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

- that the Internet must be used only for peaceful purposes
- that offensive cyber-attacks include any form of surveillance and/or eavesdropping that is not necessary and proportionate and authorized by the national courts of the target of the surveillance
- not to conduct, procure, or promote offensive cyber-attacks, in particular those that target private parties or critical infrastructure
- to limit their cyber-war research and capabilities, and their cyber-operations to purely defensive means, which do not include counterattacks
- not to produce, procure, or favor the production of tools and/or malware that can be used for offensive cyber-attacks
- to assist all efforts to detect, contain, respond to and recover from cyber-attacks
- to report any vulnerabilities than they learn of to vendors
- to follow up with vendors to ensure that known vulnerabilities are cured
- not to stockpile, sell, or exploit any vulnerabilities that they learn of that could be used for offensive cyber-attacks

11 March 2017

JustNetCoalition.org

info@JustNetCoalition.org