UDC 342.738(477)

Oleksii Barbashov,
cadet of faculty No. 4 of Kharkiv National University of Internal Affairs

Foreign experience in combating cybercrime as exemplified by the USA and Japan

Cybercrime – a catch-all term loosely defined as any offence committed using a computer or network – has exploded over the past five years. It now costs the world economy between $100bn and $500bn a year, according to the US Center for Strategic and International Studies, as more and more services are offered online, increasing the volume of sensitive data held electronically. According to the World Economic Forum's Global Risks 2012 report, cyber-attacks are now one of the biggest threats faced across the globe. Cybersecurity is becoming more important to the economic, security, and social well-being of both the United States and Japan. Cybersecurity-related solutions will need significant amounts of public-private cooperation. This includes education for citizens, the workforce, and management. Despite pronouncements by senior officials, many still do not see cybersecurity as a priority. However, people in both countries understand the need for counterterrorism and disaster preparedness, and cybersecurity can be related to these.

U.S. Government (USG) activities and its organization for cyberspace operations are based on a strong set of recent foundational cybersecurity documents, which cover both steady state and crisis response approaches. These include:

1. The Cybersecurity National Action Plan (CNAP), issued in February 2016;

2. Presidential Policy Directive-41 (PPD-41) United States Cyber Incident Coordination, of July 26, 2016;

3. A draft National Cyber Incident Response Plan (NCIRP), mandated by PPD-4110;

Current USG Divisions of Responsibility: There is a National Cybersecurity Coordinator who has regular access to the President. National policy coordination on specific issues is done through the Principals and Deputies Committees of the National Security Council (NSC). The Department of

Homeland Security (DHS) is responsible for cybersecurity on most USG networks (the Intelligence Community protects its most sensitive networks and Department of Defense (DoD) protects some of its own). The Federal Bureau of Investigation (FBI), part of the Department of Justice (DOJ), has the responsibility for prosecuting cybercrimes. The National Security Agency (NSA), reporting both to the Secretary of Defense and the Director of National Intelligence (DNI), has the greatest technical capability of any organization in the USG on cybersecurity. It provides intelligence concerning potential and actual cyberattacks that it gathers outside the United States, as well as providing technical support to other government departments and agencies when requested.

It should be mentioned, to date, Microsoft has focused most of its energies on fighting botnets: networks of computers infected with malicious software that are controlled remotely. In December, the DCU successfully partnered with Europol's European Cybercrime Centre and Germany's Bundeskriminalamt's Cyber Intelligence Unit to crush the notorious botnet ZeroAccess. The takedown marked Microsoft's eighth anti-botnet action in three years.

Several innovative initiatives are underway to improve U.S. and Japanese collaboration on military networks. Today there is connectivity on several channels, such as NIPRNET (Non-Classified Internet Protocol Router Network), SIPRNET (Secret Internet Protocol Router Network), CENTRIXS-J (Combined Enterprise Regional Information Exchange System-Japan) and others. The United States is establishing a Mission Partner Environment (MPE) to promote multinational information sharing (MNIS) globally with allies and coalition partners within communities of interest (COI).

In sum, the next few years offer great opportunities to improve cybersecurity in both Japan and the United States, but also add significant risks if the chances to fix weaknesses are ignored. So, sticking to these measures above, countries like Ukraine can take a new level of fighting cybercrime.

Received 29.10.2019