https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1028&context=ojjdp (дата звернення 12.10.2020).

2. Curry, G. D., and Decker, S. H. 1998. Con-fronting Gangs: Crime and Community. Los Angeles, CA: Roxbury. URL: https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1028&context=ojjdp (дата звернення 12.10.2020).

Дзюба Ю., здобувач ступеня вищої освіти Національної академії внутрішніх справ
Керівник з мови: ***Могилевська В.***

CANADA: CYBER THREATS AND WAYS TO PREVENT THEM

Cyber-espionage, cyber-sabotage, cyber-foreign-influence, and cyber-terrorism pose significant threats to Canada's national security, its interests, as well as its economic stability. Cyber threat actors conduct malicious activities in order to advance their geopolitical and ideological interests. They seek to compromise both government and private sector computer systems by using new technologies such as Artificial Intelligence and Cloud technologies or by exploiting security vulnerabilities or users of computer systems. Such activities are collectively referred to as "Computer Network Operations", or CNOs. State-sponsored entities and terrorists alike are using CNOs directed against Canadians and Canadian interests, both domestically and abroad. Canada remains both a target for malicious cyber activities, and a platform from which hostile actors conduct CNOs against entities in other countries.

State-sponsored cyber threat-actors use CNOs for a wide variety of purposes. These include theft of intellectual property or trade secrets, disruption of critical infrastructure and vital services, interference with elections, or conducting disinformation campaigns. In addition, non-state actors such as terrorist groups also conduct CNOs in order to further their ideological objectives such as recruitment and distribution of propaganda.

Canada's National Cyber Security Strategy views cyber security as an essential element of Canadian innovation and prosperity. CSIS, along with partners, particularly the Communications Security Establishment's Canadian Centre for Cyber Security, plays an active role in shaping and sustaining our nation's cyber resilience through collaborative action in responding to evolving threats of malicious cyber activity.

According to reports from the Canadian Security Service, the most popular cybercrimes in Canada are:

1. Violent Extremists and Terrorists

Religiously Motivated Violent Extremism (RMVE)

Ideologies that underpin RMVE often cast an individual as part of a spiritual struggle with an uncompromising structure of immorality. RMVE ideologies assure their adherents that success or salvation – either in a physical or spiritual realm can only be achieved through violence.

Politically Motivated Violent Extremism (PMVE)

PMVE narratives call for the use of violence to establish new political systems – or new structures and norms within existing systems. Adherents focus on elements of self-determination or representations rather than concepts of racial or ethnic supremacy.

Ideologically Motivated Violent Extremism (IMVE)

IMVE is often driven by a range of grievances and ideas from across the traditional ideological spectrum. The resulting worldview consists of a personalized narrative which centres on an extremist's willingness to incite, enable and or mobilize to violence. Extremists draw inspiration from a variety of sources including books, images, lectures, music, online discussions, videos and conversations. Examples of such extremism: Xenophobic Violence, Anti-authority Violence, Gender-driven Violence.

2. Espionage and Foreign-Influenced Activities

These activities are almost always conducted to further the interests of a foreign state, using both state and non-state entities. Espionage and foreign-influenced activities are directed at Canadian entities both inside and outside of Canada, and directly threaten Canada's national security and strategic interests.

These threats continue to persist and, in some areas, are increasing. Canada's advanced and competitive economy, as well as its close economic and strategic partnership with the United States, makes it an ongoing target of hostile foreign state activities. Canada's status as a founding member of the North Atlantic Treaty Organization (NATO) and its participation in a number of multilateral and bilateral defence and trade agreements has made it an attractive target for espionage and foreign interference.

Canadian interests can be damaged by espionage activities through the loss of sensitive and or proprietary information or leading-edge technologies, and through the unauthorized disclosure of classified and sensitive government information. A number of foreign states continue their attempts to covertly gather political, economic and military information in Canada. Multiple foreign states also target non-government organizations in Canada–including academic institutions, other levels of government, the private sector and civil society–to achieve these goals.

Foreign governments also continue to use their state resources and their relationships with private entities to attempt foreign interference activities in Canada. These activities are carried out in a clandestine or deceptive manner and can target communities or democratic processes across multiple levels throughout the country. Foreign powers have attempted to covertly monitor and intimidate Canadian communities in order to fulfill their own strategic and economic objectives. In many cases, clandestine influence operations are meant to support foreign political agendas—a cause linked to a conflict abroad–or to deceptively influence Government of Canada policies, officials or democratic processes.

There are ways to overcome these threats:

1. The Privacy Act (hereafter the “Act”) came into force on July 1, 1983. Under subsection 12(1) of the Act, Canadian citizens, permanent residents and individuals present in Canada have the right to access personal information that is under the control of the Government of Canada. This right of access is balanced against the legitimate need to protect sensitive information and to permit effective functioning of government, while promoting transparency and accountability in government institutions.

In addition, the Act protects an individual’s privacy by preventing others from accessing his or her personal information, and manages the collection, retention, use and disclosure of personal information.

Section 72 of the Act requires the head of every government institution to submit an annual report to Parliament on the administration of the Act during the fiscal year. This report describes how the Canadian Security Intelligence Service (CSIS) administered the Act throughout the 2018-2019 fiscal years.

2. Canadian Security Intelligence Service

In 1984, the Government of Canada passed an Act of Parliament for the creation of a civilian security intelligence service. This legislation not only gave birth to CSIS, it also clarified the differences between security intelligence activities and law-enforcement work, bringing to an end the 120-year interlocking of Canada's security intelligence service with the federal police force. CSIS came into existence on July 16, 1984.

CSIS is at the forefront of Canada's national security establishment and as such, its programs are proactive and pre-emptive. Its role is to investigate activities suspected of constituting threats to the security of Canada, and to report on these to the Government of Canada. CSIS may also take measures to reduce threats to the security of Canada in accordance with well-defined legal requirements and Ministerial direction. Key threats include terrorism, espionage, foreign interference, the proliferation of weapons of mass destruction and cyber-threats against critical information systems and infrastructure.

Through its Security Screening Program, CSIS provides advice that prevents non-Canadians who pose security concerns from entering Canada or receiving permanent resident status or citizenship. CSIS also helps prevent individuals of security concern from gaining access to Canadian information, assets, sites or events.

Список використаних джерел

1. Canadian Security Intelligence Service https://www.canada.ca/en/security-intelligence-service.html.

2. Public Safety Canada https://www.publicsafety.gc.ca/index-en.aspx.

3. Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/opc-actions-and-decisions/research.