Сова Ю.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Василенко О.

FIGHTING CYBERCRIME AND INTERNATIONAL COOPERATION: FRANCE EXPERIENCE

New destructive practices are developing in cyber space, including criminal use of the Internet (cyber-crime), including for terrorist purposes; large-scale propagation of false information and manipulation; espionage for political or economic ends; and attacks on critical infrastructure (transport, energy, communication, etc.) for the purposes of sabotage. These cyber-attacks are characterized by the following:

a) know no border or distance;

b) are difficult to trace: it is very hard to formally identify the true culprits, who are often acting under the cover of unwitting relays (botnets) or proxies;

c) can be carried out with relative ease, with little cost or risk for the attacker. They aim to jeopardize the smooth functioning of communication and information systems (CIS) used by citizens, businesses and administrations, and even the physical integrity of infrastructure that is crucial to national security.

Cyber security covers the entirety of security measures that could be taken to defend against these attacks. The constant increase in the sophistication and intensity of cyber-attacks in recent years has led most developed countries to toughen their resilience and adopt national cyber security strategies. Let us consider the example of France.

France adopted a national cyber security strategy in 2015. This Strategy aims to accompany French society's digital transition and address the new challenges of changing uses of digital technology and the associated threats: It focuses on five goals:

a) guaranteeing national sovereignty;

b) providing a strong response to acts of cyber-crime;

c) informing the public;

d) making digital security a competitive advantage for French businesses;

e) enhancing France's voice on the international stage.

This strategy has since been supplemented by:

1) France's international digital strategy: The strategy was presented by the Minister for Europe and Foreign Affairs in December 2017. It

compiles all the strategic goals France promotes in the digital field around the three pillars of governance, the economy and security.

2) Strategic Review of Cyber Defence (in French): The Strategic Review of Cyber Defence was entrusted to the General Secretariat for Defence and National Security (SGDSN) by the Prime Minister and presented in February 2018. It sets out a doctrine to manage cyber crises. This review clarifies the goals of a national cyber defence strategy and confirms the relevance of the French model and the primary responsibility of the government in this field.

Many players contribute to the efficacy of this French approach from technical and operational standpoints.

The French Network and Information Security Agency (ANSSI) was created in 2009 and is the national cyber security authority. Acting as a genuine "first responder" in French cyber space, ANSSI is responsible for preventing (including from a normative perspective) and reacting to IT incidents affecting sensitive institutions. It also organizes crisis exercises on a national level. ANSSI currently employs 600 people and continues to grow.

The French Ministry for the Armed Forces has a two-fold mission to ensure the protection of the networks underpinning its action and integrating digital warfare into military operations. In order to consolidate the Ministry's work in this field, a cyber defence operational chain of command (COMCYBER), under the orders of the Armed Forces Chief of Staff, was created in early 2017.

The role of France's Ministry of the Interior is to combat all forms of cyber crime against national institutions and interests, economic stakeholders and government authorities, and individuals. It draws on specialized central services and the local networks of the national police, national gendarmerie and internal security forces. These forces are responsible for investigations aimed at identifying and prosecuting cyber criminals. They also contribute to prevention and outreach work with relevant audiences.

Enhancing strategic stability and international security in cyber space is a French priority. The Ministry for Europe and Foreign Affairs coordinates France's work on "cyber diplomacy". This work is carried out in a European and international framework.

Guaranteeing European strategic digital autonomy, according to the European Union, France defends an ambitious vision and the concept of the "EU's digital single market", a key aspect of our collective capacity for initiative and action.

Above and beyond these dimensions, operational cooperation needs to be stepped up between EU Member States. The aim is to establish pan-European tools to share technical information on threats, supporting preparation and rapid response in the event of cyber-attacks. The creation in 2017 of the EU Cyber Diplomacy Toolbox (CDT) to combat cyber-attacks is a full-fledged aspect of this cooperation.

Apart from, France is active in other international forums where cyber security issues are tackled.

Within NATO, France instigated the adoption by the 28 Nations of a Cyber Defence Pledge during the Warsaw Summit in June 2016. This pledge recognized cyber space as a field of operations and now commits NATO to defending itself in cyber space as it does in the land, air and maritime fields. In May 2018, France hosted the first ever Cyber Defence Pledge Conference.

On 6 April 2019, G7 Foreign Ministers met in Dinard, France, and launched a Cyber Norm Initiative dedicated to sharing best practices and lessons learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behaviour. The norms that are presented in this document have notably emerged during the previous sessions of the United Nations Group of Governmental Experts (GGE) and are a subset of the international cyber stability framework. G7 countries are committed to continuing this work and to sharing views on the full range of important recommendations that have been underlined in GGE reports.

At the OSCE, which has established itself as a key regional forum for defining and implementing confidence-building measures for cyber space, France continues to promote an ambitious agenda for the effectiveness of these measures to enhance transparency, cooperation and confidence between the Organization’s member countries.

In conclusion, it is important to say, that the trend of modernization of the modern world, the ability to protect the borders of cybernet works in Ukraine are very promising and enough important, including insurance of the information preservation and preventing cyber-attacks or other malicious acts against cybersecurity in Ukraine. France's experience is an important component and effective basis for the cyber-crime protective operations in Ukraine.

If we start paving the way now, it will help avoid baffling problems in the future, possibly in the near future.

Список використаних джерел:

1. Strategic Review of National Defence and Security December 2017 by the Ministry for Europe and Foreign Affairs.

2. France's international digital strategy December 2017.
3. Digital report «Cyber Readiness France 2.0: Cybercrime and Law Enforcement» by the Melissa Hathaway.

Сокирко М.,
здобувач ступеня вищої освіти бакалавра
Національної академії
внутрішніх справ
Консультант з мови: Хоменко О.

CRIME PREVENTION DURING A GLOBAL PANDEMIC

Since March 2020 the COVID-19 pandemic has drastically changed the world. It has not only claimed more than a million lives, but it has also pushed millions of people into extreme poverty, and it has triggered a decline in human development for the first time since 1990 [1].

So, Vienna, September 2020 – Before the outbreak of COVID-19 worldwide, one in three women experienced physical or sexual violence, mostly by an intimate partner [3].

In the past 12 months, since the beginning of the COVID-19 pandemic, intimate partner violence reports have risen sharply across the globe, with calls to helplines increasing five-fold in some countries [4]. As lockdown measures were put in place to contain the spread of the virus, women with violent partners increasingly found themselves isolated from people and resources that could help them. The post-pandemic economic impact has further limited women's opportunities to escape violent situations. This "Shadow Pandemic", as defined by UN Women is "growing amidst the COVID-19 crisis" and victims, as well as survivors have limited information and awareness about available services and limited access to support services [3]. Women and girls are now often 'locked down' with their abusers, cut off from family and friends, and police and justice services are under pressure to ensure women and girls can access support, especially when traditional pathways have been shut down due to restrictions or social distancing measures [4].

Police have had to shift their focus to enforcing quarantines and increasingly severe 'stay at home' measures, and many courts have had to close completely, resulting in postponed hearings and a backlog of cases. With so many police resources needed to ensure public health measures are followed, protection orders may not have been enforced [4].

So, February 2021 – The United Nations Office on Drug and Crime (UNODC), in partnership with UN Women and the International