

3049527/Animal-cruelty-complaints-soar-RSPCA- investigates-nearly-160-000-cases-2014-one-eight-involving-violence.html

3. Cruelty to animals [Electronic resource] - Mode of access: https://en.wikipedia.org/wiki/Cruelty_to_animals#Europe

4. Animal Protection Police [Electronic resource] – Mode of access: <https://www.fairfaxcounty.gov/police/specializedunits/animalprotectionpolice>

Нагорнюк Л.,

курсант ННІ № 3 Національної академії внутрішніх справ

Консультант з мови:

Богуцький В.М.

THE VARIOUS ILLICIT USES OF CYBERSPACE AMOUNTING TO A SYSTEM-LEVEL CHALLENGE TO SOCIETY

Any analysis of cyberspace and the security threats it entails should first acknowledge that this is not the concern exclusively of governments and public authorities, commercial enterprises, or individuals. Cyber security is a problem which concerns everyone, particularly as society becomes ever more dependent on the global ICT (Information and Communications Technology) infrastructure, and therefore vulnerable to interference by adversaries able to act within or against ICT systems. In cyberspace, different interests and constituencies are challenged by a variety of interconnected actors and actions. And if society – for all its diversity – cannot respond in a similarly interconnected way, then the sum of security diminishes overall.

The challenge of cyber security can be described in terms of a spectrum of cyber threat domains: state-sponsored cyber attacks; ideological and political extremism; serious and organized crime; and lower-level / individual crime. Lower-level and individual crime such as computer hacking can appear trivial and to lack organization, but it can have high-level consequences and can feature prominently elsewhere on the spectrum. Serious and organized criminal misuse of the global ICT infrastructure is increasing, in both quantitative and qualitative terms, and at considerable cost to the global economy.

The Internet seems to fit the requirements of ideological and political extremists particularly well, and governments can expect access to and use of the global technological commons to remain closely contested. Finally, for some states and governments it is clear that the Internet is seen as a strategic asset to be used for the purposes of national security, and perhaps

more simply still as a battlefield where strategic conflict can be won or lost. The key observation here is not simply that society's increasing dependence on ICT infrastructure creates vulnerabilities and opportunities to be exploited by adversaries, but also that ICT has an increasingly important enabling function for serious and organized crime, ideological and political extremism, and state-sponsored aggression. In other words, society's adversaries are also ever more dependent upon ICT systems, creating a counterbalancing set of vulnerabilities.

Society faces considerable risk from and within cyberspace, and it must respond appropriately. Whether it does so in the form of a national cybersecurity regime or by some other means, the response must be as effective, as efficient and above all as agile as possible. Yet dealing with the problem of cybersecurity is as much a matter of the quality and comprehensiveness of the response as it is one of identifying and countering cyber threats. In important respects, the quality of the response will be determined by process and procedure, by effective coordination and by timely decision-making. But cybersecurity also poses complex structural challenges which society must address in all sectors and at all levels. How (and on what authority) should responsibility for cybersecurity be distributed between the private (individual), commercial and governmental domains? As far as public policy is concerned, which government department should be charged with developing and articulating policy, and which departments should take ownership of the various aspects of the cyber security challenge?

Addressing such questions effectively requires a close and mutually supportive engagement by a triumvirate of key actors: policy-makers at various levels of government, technical experts – the so-called "technorati" – and not least all lawful users of the global ICT infrastructure. Society must have the knowledge, the agility and the resilience to meet and preferably to anticipate the constantly evolving challenge of cybersecurity.

Список використаних джерел

1. The Law Dictionary [Електронний ресурс] Режим доступу: <http://thelawdictionary.org/article/countries-with-the-lowest-crime-rate-in-the-world> (дата звернення 24.11.2018 р.).

2. Crime and Punishment in Singapore [Електронний ресурс] Режим доступу: <https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0309cyberspace.pdf> (дата звернення 24.11.2018 р.).