Peace Research Center Prague

Policy Brief 008

July 2020 www.prcprague.cz

Double Standard on Due Diligence in Cyberspace

Tomáš Bruner

During COVID-19 lock-downs the number of cyber incidents grew approximately by one third. Hackers exploited heavy reliance on ICT technologies as well as fear within society. They targeted e.g., World Health Organization, attacked hospitals for ransom, or interfered with systems of Australian government, which was allegedly supported by another country. Warnings of national cyber security authorities repeated phrases about cyber hygiene, resilience, and prevention; simply about the necessity to exercise due diligence in cyberspace. But this due diligence seems to be a tricky double standard, which could have unpleasant consequences.

The principle of due diligence requires that one does not allow his/her cyber infrastructure to be used in a way that harms others. It is extremely helpful for dealing with situations where a perpetrator can be hardly identified. The logic is simple. If you cannot catch and punish the thief, you can still sanction someone who negligently left the door unlocked. Applied in cyberspace, if you cannot catch the hacker, just sanction those who allowed him/her to conduct the strike, because they did not adopt sufficient precautionary measures.

Unfortunately, the application of this principle differs on national and international level. Under national law, States strictly require companies and private persons to exercise due diligence in cyberspace, especially in regard to personal data. Internationally, States are reluctant to accept due diligence obligation themselves and question its applicability. As a result, governments can easily sanction negligent behaviour on national level, but the same governments rely that under international law, they cannot be sanctioned for negligence which allowed a cyber strike to stem from infrastructure under governmental control.

This double standard might be illustrated by the attitude of the UK. In Summer 2019, hackers diverted the visitors of British Airways websites to a false interface and thus stole personal data of approximately 500.000 customers. Although British Airways was the victim not the perpetrator of the incident, the company was fined £ 183 million for negligence: insufficient protection of personal data. For similar reason, Marriott Hotels group

About the author

Tomáš Bruner is a lawyer (compliance officer) in private corporate sphere, teaching assistant at the Charles University and a researcher at the PRCP.

in the UK faced the fine of nearly £ 100 million. The corporation had acquired a new network of hotels which had a computer system compromised by hackers at the time of acquisition. Marriott failed to discover it and to stop the unlawful data drain. Both decisions emphasized that companies must exercise due diligence and thus prevent any harmful behaviour in regard to personal data in cyberspace. Paradoxically, only year earlier, British Attorney General Jeremy Wright pleaded that under international law, there was no obligation of due diligence which would bound the UK or other governments. Due diligence principle thus proved to be an effective domestic lash against negligent companies, while it seemed toothless internationally against negligent governments.

Estonian Prime Minister Jüri briefs the UN Security Council on the relationship of global pandemic and security in cyberspace, May 22, 2020.

Source: Estonian Ministry of Foreign Affairs

This disparity became even more visible during corona crisis. The EU Agency for Cyber-security, US Cyber-security and Infrastructure Agency and other national authorities issued warnings that private companies must be extremely cautious in cyberspace. At the same time, international debates whether due diligence applies also on States in cyberspace remained stuck in a deadlock. In 2013 and 2017 two expert manuals (Tallinn Manual 1.0 and Tallinn Manual 2.0) composed by lawyers specified that the States should not knowingly allow their cyber infrastructure to be used in a way harmful for other States. Hpwever, this rule met with mixed reaction of governments and even the authors of Tallinn manuals were not able to specify what exactly this means. The international laws of cyberspace were examined also by UN expert group. Nonetheless, the work of this group has been recently paralysed by lack of consensus. Finally, the EU adopted the regulation of cyber-sanctions in 2019. Under this regulation, physical persons and companies may be sanctioned for perpetrating a cyber-attack. The regulation does not specify whether a State can be also responsible for a cyber strike or for negligence that facilitated it. So, can the principle of due diligence be overlooked by governments on international level, although it is rigorously applied on national level?

It should not. Public international law is contained in various sources: in international legal customs, treaties, and also in general principles of law. General principles of law include rules common to major legal systems of the World. Although there is neither an international treaty nor a custom directly regulating due diligence in cyberspace, States should not pretend that due diligence in cyberspace applies only domestically. Once cyber due diligence becomes part of national legal regulation contained in a system(s) such as common law or continental law, it also transforms into a general principle of international cyber-law.

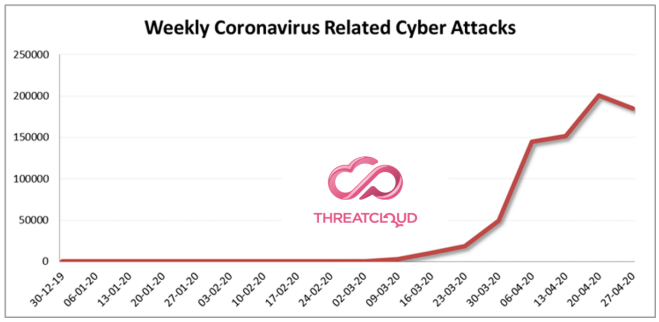
And due diligence is indeed becoming widespread national rule in cyber space. This can be demonstrated on three areas: personal data protection, responsibility of companies, and cyber insurance.

In 2016, the EU adopted General Data Protection Regulation (GDPR), which is directly applicable for all EU members. It demands that anyone processing personal data in cyber- as well as physical space implements effective technical and organizational measures for their protection. Because of so called "Brussels effect", other countries started to adopt regulation similar to GDPR. In 2020, Consumer Privacy Act entered into force in California. According to the US Federal Trade Commission, a company's failure to secure personal information in cyberspace represents a deceptive and unlawful practice. In 2019, Indian Parliament approved Personal Data Protection Bill and even China is preparing new data protection regime as a part of new Civil Act. The obligation to exercise due diligence in regard to personal data in cyberspace becomes omnipresent under national law.

Correspondingly, companies are usually required by national law to exercise due diligence to prevent unlawful behavior of their employees. Otherwise they can be found liable for crimes that their employees committed in course of their work, including crimes in cyberspace. Finally, also the commercial market acknowledged the requirement of due diligence in cyberspace. In recent years, the popularity of cyber insurance grew. Global insurance groups like Aviva, AIG, VIG, AXA, Generali, Hiscox or Zurrich started offering this insurance, which covers e.g., reputation damage or fines imposed because of a failure to exercise due diligence. The importance of cyber-insurance has been emphasized by OECD, EU-US dialogue, or European Insurance and Pensions Authority.

In a nutshell, cyber due diligence is being globally embedded in national regulation of personal data protection and liability of companies, while also private sector recognizes this obligation by selling respective insurance. This is a robust basis which allows national due diligence to grow into a general principle of international cyber law.

Governments understandably fear that inter-state application of due diligence in cyberspace could bring disadvantages. It would be burdensome for countries with high malware infection rates and restrictive for countries illicitly supporting cyber espionage and harassment. However, general principles of international law are formed regardless of State fears or awareness. Thus, the requirement of due diligence in cyberspace can suddenly enter international law and bind governments in international relations, because most of them fostered it domestically. After all, it would be hypocritical if governments punished negligence under national law and overlooked their own negligence under international law.



Coronavirus-related attacks, detected across networks by private ICT security tech provider Check Point.

Source: blog.checkpoint.com

Instead of ignoring or opposing it, governments should prepare for the option that due diligence becomes part of public international law. They should focus on how it

applies rather than whether it applies. Otherwise they might be unpleasantly surprised. Sooner or later, someone will invoke this principle or even hijack it to serve particular interest. And without exact specification how should due diligence apply in cyberspace, it could do more harm than good at least in five regards:

1. Thresholds: it must be specified, what types of incidents are so serious that they must be prevented by governments and what other types fall below *de minimis* threshold. The distinction must be proportionate to states' individual capacities. Otherwise, due diligence would truly become too burdensome.

2. Countermeasures: if State A fails to avert a cybers-trike by exercising due diligence, State B shall be entitled to countermeasures against State A. It should be specified which countermeasures are appropriate for various incidents and how long can they last. Otherwise, due diligence could become a tool of provocation and destabilization. Through spoofing, hackers can steel IP addresses and hide behind someone's identity. This could be misused to spark or escalate conflicts.

3. Triggers: it should be clarified whether states must act preventively just with a constructive knowledge that a cyber-attack might stem out from their infrastructure, or whether they must act only with actual knowledge that cyber-attack already commenced from this infrastructure. Unless this is clarified, states will choose between the two options as they wish. Some might recall the former option to justify domestic monitoring activities or to intentionally over-burden other states. Others might insist that the latter option applies in order to avoid responsibility.

4. Human rights and freedoms: it should be specified how requested due diligence affects individual rights so that due diligence does not become a disguise for restrictions on freedom of speech or right to privacy.

5. National implications: it should be specified what consequences can the lack of due diligence of State A have under national regulation of State B. State A cannot be sued by a national court of State B. But the damaged citizens and entities in State B can sue particular person, e.g., government member, of State A. This tactic sometimes called "attribution by indictment" has become popular in the United States. The US legislation contains also the possibility of class action (group lawsuit), where many victims may sue an offender for a similar claim. The same legislation is being adopted in the EU and called the Directive on representative actions for the protection of collective interests of consumers. As a result, if a future cyber-attack affects huge number of persons, they may file a class action against a person within governmental structure for the negligence that allowed the cyber-attack to happen. Such class actions could be an interesting business for law firms that would subsequently rally victims of such cyber-strikes in an attempt to win damages and earn success fees. And national courts and government would have to deal with an unprecedented yet very real situation.

Those are the issues that governmental experts should address instead of defending the position that due diligence in cyberspace does not apply on States under international law.