PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 32 (485), 26 March 2013 © PISM

Time for an International Law on Cyber Conflicts

Rafał Tarnogórski

In cyberspace, the line between peace and war becomes blurred. At the same time the protection of the network infrastructure is becoming one of the key strategic objectives in the area of national security. Cyberspace can be used for a terrorist attack or an attack on a scale comparable with a military attack, but there is no treaty relating to military operations in cyberspace. The development of an international convention relating to cyberspace is in the interests of the international community.

The use of cyberspace for espionage and military offensives is the subject of constant and growing interest for the armed forces and intelligence organisations of various countries. In recent weeks, news spread around the world about the discovery of unit no 61398, located in Shanghai and part of the Chinese People's Liberation Army. The unit is, allegedly, responsible for a campaign of cyber espionage against public agencies and commercial companies in the U.S. and Europe. Even if this allegation is not confirmed, it is certain that China—like all powers—has this type of agency, tasked to plan, prepare and conduct offensives in cyberspace. All large-scale cyberattacks have been alleged to have been state operations. The popular media linked the paralysis of the internet in Estonia and the blockade of Georgian websites during the Russian–Georgian war in 2008 to Russian secret services. The Stuxnet worm, detected in 2009, was commonly seen as a joint American-Israeli effort to sabotage the Iranian nuclear programme. The latest cases of Flame, Mahdi or Red October (2012) malicious software, which let unidentified perpetrators steal huge amounts of data from American and European government and commercial networks, were linked to state actors not only by media but also by information security experts. Yet, the very nature of cyberspace makes it difficult to attribute attacks in all cases. This is both a key challenge for cybersecurity, and an incentive for states to seek methods of using electronic attacks for espionage and military offensives.

The Rise of the "Cyber" Battlefield. Cyberattacks became part of the arsenal of weapons used on the modern battlefield at the very same time that the notion of the battlefield itself was transformed. Following the terrorist attacks of 11 September 2001, the United States responded by declaring war on terrorism, using conventional means against an assymetric threat. At roughly the same time, security experts started to indicate that information technology could also be used to conduct an attack, the effects of which could be comparable to conventional armed aggression.

As in the case of the fight against terrorist organisations, conventional legal rules governing armed conflict can hardly be applied to cases of cyberattacks, and require redefinition. At the same time, the need to protect electronic networks, being an integral part of the infrastructure of the state, is not in any doubt. Some states have already declared that they are ready to respond to the most severe cyberattacks using traditional military means. The United States, with its 2011 strategy on cyberspace, is one such nation, but the term "cyberattack" also appears in strategic documents of other states, including the UK, Canada and Russia, and in the Polish government's official Republic of Poland Cyber Security Programme for 2011–2016.

The Need to Establishing Legal Rules. Cyberspace has a public dimension which requires legal protection, also through international regulations. This dimension covers not only critical infrastructure (networks used by, for example, the financial sector, automated transport systems, electricity, gas and oil delivery systems) but also internet-

based commercial and public services (e-administration). Providing security for those systems and services is especially significant in the case of large scale cyberattacks, giving rise to the idea of the treaty regulating cyberspace.

In March, the Tallinn Manual on International Law Applicable to Cyber Warfare was published at the request of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. The book examines in detail the legal problems associated with the law of armed conflict in cyberspace. This is not a collection of binding international law, but only suggested solutions, and even in the opinion of the authors themselves these suggestions may yet change. However, despite some objections, the Tallinn Manual could establish a legal framework for military actions in cyberspace, because the recommendations presented in the document will be taken into account when creating national legislation. The main achievement of the Manual is showing the gaps in international legislation, such as how to avoid indiscriminate attacks in cyberspace and when an act of cyber hostility begins.

The Tallinn Manual addresses the need to establish new rules, because those that already exist do not include the new cyber circumstances, although they can sometimes be applied by analogy. In example, the UN Charter recognises the inherent right of self defence in the case of an armed attack, until the UN Security Council takes action to establish international peace and security. Whether a cyber operation constitutes an armed attack depends on its scale and effects. There are also limits to using self defence in response to such a cyberattack. The principles of necessity and proportionality, in the context of a particular case, are crucial aspects that influence whether an action is indeed taken in self defence. The use of military force as a consequence of cyberattack is not prohibited by international law, but its legitimacy will be assessed on the basis of the above criteria. Therefore, it seems that a cyberattack directed on critical infrastructure of the state can be legally recognised as an act of armed aggression entailing conventional retaliation.

But states do not have full freedom as regards military action in cyberspace, as they are still subject to the applicable rules, even if those rules are imperfect. International humanitarian law as set down in the Geneva Conventions are applicable in case of any armed conflict, even if it is not classified as a state of war. The rules, where appropriate, also apply in the case of armed conflict that is not international in character. Therefore, in light of the humanitarian law, a cyber war would be treated as any other armed conflict. This statement entails serious consequences. Humanitarian law defines the protected categories of persons and property during hostilities. A serious violation of the laws applicable in armed conflict could lead to an individual being held criminal responsible for a war crime. So an unlawful cyberattack on civilian infrastructure under such protection, such as hospitals, should be considered a war crime, and those responsible prosecuted, including through the International Criminal Court.

Conclusions. There is no binding international treaty on military operations in cyberspace. This gap would not be filled by the Tallinn Manual. It requires systematic regulation, set forth by a internationally binding legal document, a multi-lateral convention related to cyberspace. It is in the best interests of the international community is to develop a robust set of legal principles, governing the actvities of states in cyberspace, for example defining the lawful object of cyberattacks, when hostilities begin in the cyberspace, who is protected by law, and what activities are strictly prohibited. Work on this subject should come under the auspices of the International Committee of the Red Cross. The relevant legal principles should be developed by the International Law Commission, as a recognised authority in the field of progressive development of international law. The development of such a document in the form of a binding act of international law does not interfere with Polish interests. The legislative work on a draft convention could gain broad international support from NATO allies and the EU, but also from Russia and China (which, in 2011, put forward a proposal to develop an International Code of Conduct for Information Security).

In Poland, a plan to protect curcial networks against cyber threats was included in the abovementioned Republic of Poland Cyber Security Programme for 2011–2016. It defines the legislative framework (the need to identify new areas of activity, responsibility, and changes in the organisational structures of state bodies and cyber security agencies), procedural and organisational issues (in particular the role of CERT.GOV.PL and the planned Inter-ministerial Group for the Protection of Polish Cyberspace), and technical protection. However, the military aspects of security were not in the scope of the document. Poland should build cyber capabilities based on military structures as soon as possible, including tools for an adequate response to serious violations of Polish cyberspace by any means necessary means, including the threat or use of force.