



LEGAL PROTECTION AGAINST UNLAWFUL CYBER OPERATIONS

by Anton Kim

COLIBRILAW



Imagine that you are a citizen of a Central Asian country. Now, not only are you a national of the country, but you actually live in Central Asia and own a highly profitable online business, which operates from a website located on a server within the European Union. Everything seems fine when, all of a sudden, malicious software wipes out all the data on your website, but not before the perpetrator of the attack duplicates its content. Appalled and devastated by the severe damage done and the boldness of the perpetrator, you seek justice and retribution.

What we will examine here is whether there is a legitimate way for someone in this situation to obtain retribution.

Introduction

Information has always meant the difference between triumphant success and miserable failure. However, never before has the importance of information been as evident as it is today. Almost everyone is dependent on the Internet in a way that was previously inconceivable. As such, today information is volatile, rapid and, most importantly, abundantly accessible. However, such benefits could not come without a price. Although information is now more fluid and accessible, it is also vulnerable and fragile, for the Internet is often far from friendly and safe.

Academic circles have aptly described the Internet as the Wild West of our age, where national borders are murky, laws are barely enforceable and users are safe from the lunging grip of the authorities. This state of affairs propagates a certain atmosphere amongst some Internet users and it would not be an exaggeration to state that the spirit of impunity reigns freely, with users free to indulge in doing whatever they wish. Indeed, the actions of an ill-intentioned few are at odds with most national and international laws.


Understanding the *modus operandi* behind Cyber Operations

The most popular weapon of choice for wreaking damage on the Internet is Cyber Operations (CO). COs are capable of almost anything, from bringing down nuclear reactors and taking control over the US Air Force missile drones, to stealing precious intellectual property from corporate entities and replacing users' profile pictures with offensive imagery. Purely technical means of protection against the onslaught of COs are, of course, available, ranging from the most rudimentary "firewalls", which deny unauthorised access to a computer, to complicated backfiring engines, which literally "hack back" the wannabe hacker. However, no contemporary security system can provide a 100% safety guarantee against COs. Every computer programme, including security systems, has inevitable vulnerabilities, leaving them open to exploitation by malicious users. Therefore, for those behind the COs there is always a way to get around cyber defences, no matter how complicated they are. As such, anything somehow connected to the Internet is at constant risk of cyber assault.

Another important feature of COs is their *modus operandi*. As they use the most modern technologies, COs pose an advanced challenge to laws, many of which date back to the days of the Roman Empire. Most laws aimed at tackling the threat of COs stem from the legal principles that were designed to punish non-cyber crimes such as burglary and theft, and, as such, could not possibly have foreseen either the advent of the Internet or the crimes committed within the digital sphere in the modern age. Therefore, in order to understand legal protection against COs we must first understand the *modus operandi* behind them.

Before we proceed any further, we should first examine what COs actually are. Generally, COs can be defined as actions committed in cyberspace with the aim of achieving a variety of effects, including (1) the erasure/corruption of data on a network or a system connected to that network, (2) becoming an active member of a network and subsequently producing forged information traffic, (3) the covert alteration of data contained in a network, (4) the disruption or denial of a service on a network. Put simply, a successful CO consists of two key elements: (a) activities completed in cyberspace (including the screening or tracing of data, etc.) and (b) the effect resulting from such activities.

The activities themselves are not unlawful *per se*. However, the effects of COs are open to the application of law and could therefore potentially be considered unlawful, thus rendering the entire CO unlawful. This effectively means that the law applies to COs in a *post-factum* way. Thus, until the effect of the CO manifests itself, it is impossible to commence the legal analysis of a CO, or to determine whether it violates the law. Not only does this leave the perpetrators space to practice guiding COs from the initiation to their effects, but it also bars any legal action until the unlawful effects of COs come into fruition.



In view of the above, the key problem regarding the legal response to COs revolves around two key aspects:

1. The ability to trace perpetrators – in order to even attempt to bring legal action against the perpetrators of unlawful COs, the authorities must first locate them. Cyberspace is both vast and global. However, if an Uzbek national can download pictures of cute cats from a server in the USA, the same applies to an individual in the USA attempting to access Uzbek servers. This effectively means that COs can be executed from anywhere in the world to anything or anyone in the world, provided the target and the perpetrator are interconnected (usually via the Internet).

Every computer and computer network (CN) connected to the Internet possesses a unique Internet Protocol (IP) address, which contains information crucial for locating the whereabouts of the computer or CN and, in turn, the individual operating this computer.

However, IP addresses can be masked and even feigned. In addition, the Internet offers the possibility of outsourcing the commission of COs, allowing an individual to launch a massive CO from thousands of slave-computers around the Internet, which are simultaneously directed by the master signal of the individual (this usually applies to “denial of services” attacks). In such cases, tracing the master signal responsible for issuing the relevant command can be extraordinarily difficult, if not impossible.

2. Jurisdiction over the perpetrator – there are no legal challenges in bringing to justice an individual that has committed an unlawful CO against a target when he or she resides within the same country as the target. However, given that COs can be committed from anywhere in the world, the perpetrator may well be on the other side of the globe, where the jurisdiction of the authorities in question does not apply. Indeed, this is usually the case. Therefore, even if the authorities do manage to identify the location of the perpetrator, the usually long arm of the law might end up being too short to reach the individual responsible.

In this case, the only feasible option to attempt to bring the perpetrator to justice would be to seek the assistance of the jurisdiction where the responsible individual resides. This might be a long process if the two countries share a legal assistance agreement, or extraordinarily long if no such agreement exists between them. In addition, it is possible that the authorities of the other country might refuse to cooperate, especially when the individual concerned is a national of the aforementioned country. Even if the country of the CO is willing to assist in investigating a CO, unlawful COs may not be criminalised in the relevant national legislation, thus greatly complicating cooperation.

Legal response to the threat of COs worldwide


When confronted by the challenge of unlawful COs ravaging Internet domains, and upon realising the damage COs can do to the private and public interest, governments were relatively quick to respond to the rise of unlawful COs.

From a legal standpoint, governments' responses revolved around equipping their national legislations with laws aimed at either establishing legal protection against COs (prohibitive legal acts), or establishing criminal liability for the commission of unlawful COs. Examples of such legislation vary from the US Electronic Communications Privacy Act, dating right back to 1986, to the 2004 Data Protection Act of Mauritius.

It should be noted that although national legislation is a significant step in combatting unlawful COs, it only solves half the problem. As previously established, COs are a global phenomenon that easily traverse national borders, a fact that helps the responsible individuals to escape the grip of the law. Perpetrators of COs are often located outside of the countries of their targets, which effectively puts them outside the jurisdiction of the authorities to which these acts may be reported.

Solving the challenge of jurisdiction can be achieved either by signing a multitude of bilateral agreements between states, as outlined above, or by establishing a common legal space via a convention with (1) a universal jurisdiction over unlawful COs and (2) an obligation to assist in investigating and punishing individuals responsible for unlawful COs occurring in one of the member states of the convention (3) the obligation to criminalise unlawful COs in the national legislation of the member states of the convention, which appears to be a much better solution to the problem.

To date, the only successful and effective example of such an instrument is the Budapest Convention on Cybercrime (2001). With a membership pool of 47 states, including non-EU members such as the USA, Japan and South Africa, this Convention effectively establishes a legal space wherein (1) all possible COs committed with the intention of violating any economic rights are criminalised; (2) member states of the Convention command full jurisdiction over unlawful COs conducted within the territorial jurisdiction of any other member state of the Convention; (3) member states are obliged to provide all procedural assistance upon the request of any other member state of the convention. From a technical perspective, the Convention establishes a wide cooperation mechanism in the form of a permanently active communication processing centre, from which any assistance requests of the member states are processed around the clock and within a matter of minutes. This is certainly an effective way to bolster the tracing capacities of all member states, particularly as in the context of cyberspace, even a few missed seconds can mean the difference between locating the individual or losing his or her track.



To put it simply, adherence to this Convention by member states effectively suggests that, should an unlawful CO be committed against public or private interests within the jurisdiction (including against naval vessels, aeroplanes and overseas territories) by either a national of one of the member states or from within its jurisdiction, the relevant member state would then provide full procedural assistance and any other legal assistance required to locate the individual concerned and to bring him or her to justice. The Convention provides the effective tools required to tackle the challenge posed by the extraterritorial capacity of COs and, to some extent, responds to the technical aspect of COs. To date, this is the most efficient mechanism implemented for combatting the rise of unlawful COs on the Internet.

Protection against COs in the countries of Central Asia

To assess the level of protection afforded under the legislation of Central Asian countries we will project the properties of the Budapest Convention on Cybercrime upon the state of the legal systems of Kyrgyzstan, Kazakhstan, Uzbekistan and Tajikistan. In doing so, we will use the two most important elements of the Convention as the tools of measurement: (1) the criminalisation of unlawful COs under national legislation, (2) uniform jurisdiction over unlawful COs and a means of assistance in investigating and punishing the individuals responsible for unlawful COs that occur in one of the member states of the region.

Having conducted an analysis of the legislation of the aforementioned Central Asian countries, we have established that, given that the legal systems of the region all stem from the Soviet era, they mostly resemble one another. All four countries have legislation that establishes (1) a data protection regime and the protection of computer network systems and (2) the criminalisation of unlawful COs with possible economic consequences. However, there is no legal tool that establishes cooperation and common jurisdiction between the countries of the region, as is achieved by the 2001 Convention.

It can therefore be concluded that the countries of the Central Asian region provide limited legal protection against the threat of unlawful COs, particularly within the national borders of the country where an unlawful CO was committed.

Case Study

Finally, let us return to the hypothetical case of a Central Asian national falling prey to online predators.

Obviously, as a national of one of the Central Asian countries whose rights have been violated, you can appeal to the law enforcement authorities of your country in order to seek justice. Your country will be able to do a number of things to assist you in bringing to justice the individual responsible, as well as in retrieving the data stolen from your online business. However, all their actions will be restricted to their territorial jurisdiction, therefore preventing the authorities from directly reaching the responsible individual. Additionally, Central Asian countries have not signed any bilateral legal cooperation agreements with any of the EU nations. Therefore, in order to enlist the assistance of the EU country in which the crime took place, the Central Asian states would have to undergo an extremely lengthy process of bilateral negotiations, with no guarantee of ultimate success.

Against this background, the data was located on a server within the jurisdiction of the EU. In addition, the state exercises full territorial jurisdiction, meaning that any crime committed within its national borders (including naval vessels, aeroplanes and oversea territories) is fully subject to its jurisdiction. Territorially, the corrupted and unlawfully duplicated data was resident on an EU server at the time that the CO was carried out, which thereby suggests that the crime took place on EU soil. This therefore enables you to appeal to the authorities of the EU country in question in order to seek the protection of your rights. Most members of the EU have long-standing experience of combatting cybercrime, elaborate and time-proven technical tools far surpassing those of the Central Asian countries, and, most importantly, an agreement establishing universal jurisdiction over unlawful COs throughout the EU space. The combination of these factors will provide you with a greater chance of successfully protecting your rights, compared to the possibilities offered by appealing to the national authorities of the Central Asian countries.

Author

Anton Kim / anton.k@colibrilaw.com

Anton is a Junior Associate within Colibri Law Firm's Tashkent office. Prior to joining Colibri, Anton specialised in public international law, international humanitarian law and international human rights law, focusing particularly on the application of public international law to cyber warfare.