The Legal Framework in Central and Eastern Europe

We live in a society increasingly dependent on and enamored by technology, including communications, surveillance, forensic, health care, and other forms of technology. The cyber age has exposed sovereignty to new challenges. Cyber-attacks represent new ways of intruding on the sovereign prerogatives of states. As usual, the law has struggled to keep pace with technology.

Countries of Central and Eastern Europe have generally made less progress in reforming their legal systems to incorporate cybercrime, though Russia stands as an exception. Russia has developed an extensive legal framework to detect, punish, and prevent computer crime, but implementation remains problematic.

While Communism ended in most parts of Eastern/Central Europe and the former Soviet Union over several decades ago, the legal and judicial systems in many of these nations seemingly defy reform efforts. Despite vastly different conditions in these countries, the Western nations’ cookie cutter approach to import and apply Western legal concepts to assist with legal reform in the former Communist world despite the vastly different conditions in these countries has failed. After the fall of communism there were great expectations in both the post-communist countries and the established West that the model that would replace communist legal framework would follow a more Anglo-American paradigm. It has taken the Anglo-American system more than 200 years to reach its current stage of development, based to a great extent on the progress and experience of several revolutionary developments. Post-communist development has only lasted several decades, the societies are in permanent flux, simultaneously fighting legacies of the past and searching for successful ways of building up the states based on the rule of law, as well as civil societies.

Self-regulatory bodies in all these countries are relatively ineffective or have little real authority. Unstable, rapidly changing societies are not the proper environment for supporting the principles of self-regulation. Even where respective laws exist, their application is often inadequate. It takes time until the legislation becomes truly operative, and the same applies to the written and unwritten conventions. There is no magic pill or quick road to legal and judicial reform in the
post-communist world. Bringing change to these societies, as to any society, will take time, patience, and consistency.

Cyber Crime in Central and Eastern Europe

Societal transformation in the post-communist countries coincided with the global revolution in information and communication technology. The crime syndicates of Eastern Europe have become masters at understanding human behavior and interaction with technology.

Many of the economies in the Former Soviet Union and Central and Eastern Europe (FSU&CEE) have become top cybercrime hotspots. Cybercrime rings in these economies have mastered complex tricks and have increased pervasiveness and sophistication of cyberfrauds. Sophisticated frauds such as cyberextortion, distributed denial-of-service (DDoS) attacks and hijacking users’ searches and clicks involve a complex fusion of strategy, technology, processes and people.

In the early days of the post-communist era, East Europeans (especially Bulgarians and Russians) have focused their attention on infecting capitalist countries as a response to the state of their economy. Aided by a solid background in mathematics and cryptography, the East Europeans have quickly become the undisputed champions in a, back then, means of political protest and retaliation. Over the past several decades, these groups have shifted their focus from political protest to writing commercial malware and their experience with malware, packing and cryptography have made a huge difference. Eastern European hackers operate in small teams, are precise and focused in their attacks and go to great lengths to protect their identities because their reputation is the key to their success.

The East European underground can be characterized as a tightly knit community of fellow mercenary commandos who routinely buy and sell data to one another, if your reliability is called into question, your ability to profit or even survive is harmed, possibly to the point of extinction. East European hackers focus on stealing data they can immediately sell or exploit for a profit, like financial credentials, credit card details or personal information. This is why the Eastern European cybercriminal underground has developed cybermoney-laundering systems that use customer vetting and alternative payment channels. They have created a "giant arms bazaar" by which criminals sell cybertools to others. They are "master craftsmen" when it comes to malware development their malware are so elegantly crafted, that they have been dubbed the 'Faberge Eggs' of the malware world. In fact the region is considered as a high-end-market with a robust economy which serves as the arms bazaar for myriad of cybermunitions and bulletproof hosting infrastructure. East Europeans act like snipers when they launch attack campaigns. The hackers in this region use exploits created by others for initial penetration, but their malware programs are customized specifically for their goals and have all of the needed functionality built in. Malware programs produced in Eastern Europe tend to be small in size and use advanced detection evasion techniques.
Corruption, the lack of sufficiently high penalties, ineffective, inefficient, inadequate and weak legislation and lax law enforcement have fuelled cybercrime in this region. Likewise, key private sector players have indirectly encouraged cybercrimes. For instance, ISPs in the region arguably have no vested interest in fighting spam consisting of ads and malware as doing so would lead to a decrease in their traffic and hence revenue.

**Cybersecurity in Central and Eastern Europe**

When it comes to Cybersecurity, Central and Eastern Europe is a region on high alert. International cooperation will be essential to a truly effective legal response. New international efforts to regulate cyber-attacks must begin with an agreement on the problem - which means agreement on the definition of cyber-attack, cyber-crime, and cyber-warfare. This would form the foundation for greater international cooperation on information sharing, evidence collection, and criminal prosecution of those involved in cyber-attacks - in short, for a new international law of cyber-attack.

"Cyber-attack," "cyber-warfare," and "cyber-crime" are frequently used with little regard for what they are meant to include. This lack of clarity can make it all the more difficult to design a meaningful legal response.

However, two things are certain. First, experience indicates that cyber threats will be propagated from those jurisdictions that criminals, terrorists, or other malicious actors find most favorable, i.e., those with the least stringent domestic regulations and the greatest inability to monitor or curtail malevolent Internet traffic. In legal terminology, that means the adversary will always have the "choice of venue," which directly implies the second truism. Namely, the ultimate solution to the systemic insecurity that is engendered by a globally connected infrastructure will not be found in the reinterpretation or reform of any particular state's legal authorities and enforcement capabilities. Similarly, unilateral declarations or actions are unlikely to resolve the common problems faced by all sovereigns. Cybersecurity has become a worldwide concern which requires the establishment of collective norms and cannot be adequately addressed by any nation in isolation.