Special Essay Contribution from the past Chief Editor

INTERNATIONAL JOURNAL OF
LAW, LANGUAGE & DISCOURSE

The Language of Cyberattacks

Phil Cameron
USA

Dr. Phil Cameron taught as professor for universities in Asia, MENA, Europe and North America. He is a United Nations legal expert and government legislative consultant for several different countries. He is an Instructor of International Humanitarian Law for the American Red Cross, The Space Travel Law Association, and serves as President of the Rule of Law Association with Certified Information Systems Security Professional, Project Management Professional and Intellectual Property credentials. www.DrPhilCameron.com

Abstract

This essay is a post-structuralist analysis of legal systems and terminology used in government-based high technology activities. In the pandemic contact tracing post 9-11 era of high technology global security, there is no single determinate structure for the application of basic international law principles. The legal terms in practice do not point at things, persons, structures, nor even at other words with reliable predictability. The novelty of the technologies used results in referent persons, locales, situations and governing laws being subject to the broadest interpretive license. Meanwhile, the originating spirit found in international legal rules protecting civilians, such as the Geneva Conventions, has been applied to electronic attacks during times of armed conflict. This essay discusses the semantic importance of "threat, crime, attack, security" language and the referent persons conducting the activities. A linguistic deconstruction of the techniques of intelligence gathering is discussed, such as packet sniffing, FBI cybercrimes investigations, data collection, remote sensing, storage and retrieval of records. This includes an analysis of the places involved in cyberattacks and digital trespass which redefine the meaning of borders through electronic security-surveillance during border entry such as airports. These surveillance, security and cybercrime concepts are grounded in a history and culture whose new laws are based on state-of-the-art applications and re-interpretations of traditionally accepted legal principles. Post-structuralism as applied to cyberlaw argues that to understand these legal referents, it is necessary to understand both the object itself and the historical technological lineage that produced the cybersecurity laws

Keywords: post-structuralist linguistics, surveillance, security, cybercrimes, international humanitarian law, international law, technology, computers, civilians during armed conflict, cyberattacks, cyberwarfare, state borders

An overview of cybersecurity under international law

Cybercrime and cyberwarfare have significant real life effects outside of the virtual world.[1] The most basic rules of cyberlaw are probably familiar and intuitive to most people:

- Certain activities are crimes regardless of whether the actions are based on virtual computer technology or tangible real world actions. “If it is illegal offline, it is illegal online” (Ugo 2005).
- Offensive cyberattacks and defensive cybersecurity rules are in place for use during armed conflict, and also for the preparation and prevention of armed conflict.
- During war, the military has a legal obligation to minimize harm to civilians. When possible, civilians must be protected during armed conflict. Harm to civilians during cyberwarfare is prohibited by international law.

In fact, it is the simplicity of these concepts that leads to great ambiguity and diverse application in practice. One remarkable characteristic of cyberattacks is that the bad guy has a high likelihood of remaining anonymous. Cybercriminals are said to “spoof” systems and as a class are referred to as a “spook” or a “ghost” denoting their incorporeal and “non-existent” presence. Hackers are talented to spoof their IP and email addresses to secretly infiltrate networks, do their dirty work, and clear the logs of their digital activities. This animosity is compounded by the fact that there is a marked lack of reporting of cybercrimes. Even though required by law to report cybercrimes that happen against their business, organization or government, most do not want to report the crime because they don’t want to lose credibility, confidence nor have their bad data and secrets become a newsworthy headline. This victim’s shame, thereby perpetuates the ethereal nature of the crime and the criminal. (The term “bad guy” is actually professional jargon in cryptology.)

Animosity makes prosecution and enforcement difficult. Spoofs traverse multiple computer systems enroute to their cybervictim. Typically, these are the computers of innocent people and businesses whose machines are being controlled by the bad guy. Entry and control are gained through introduction of malicious spyware and malware (i.e., bad guy software) embedded in websites, emails and attachments that appear as something other than what they really are, termed as a “Trojan horse.” This software, also known as “bot,” then waits in a dormant state for commands from the spoof. These controlled computer systems are referred to as robots or zombies, and a chain of them forms a “botnet.” Just as attackers have found ways to distance themselves from the crime, the number of penetrations and the level of data access and remote network control have greatly increased. The range of cyber bad guy identities spans foreign and domestic governments, military, commercial, private and criminal enterprises. A cyber bad guy could be freelance or employed by anyone.

The ambiguity of the actors continues once their identity is known. Independent cyber perpetrators may be called hackers, but there are security weakness detectives that are trained to find and correct network vulnerabilities who are certified as an "ethical hacker."[2] The exposure of data found business trade secrets, confidential personal logs, or top secret sources that implicate government crimes can be made public by the protected "whistleblower" or the wicked "traitor" to the state. Exposed bribery by public officials to induce behavior of other public officials might be seen as diplomacy, but the same bribery by private citizens would make them criminals and those government officials receiving the bribe "corrupt." The moral content of the action, it seems, depends on the identity of the actor, as much as the context of the cyberattack.

The USA Director of National Intelligence, James Clapper, at the Senate's Intelligence Committee hearing in February 2012 said that non-state actors are increasingly gaining in prominence, and in fact already have "easy access to potentially disruptive and even lethal technology." Clapper said that hacker groups like Anonymous and LulzSec have been carrying out a consistent campaign of distributed denial of service attacks and website defacements, and that intrusions into NASDAQ and the International Monetary Fund "underscore the vulnerability of key sectors of the economy" (Hoover 2012).

The International Information Systems Security Certification Consortium, Inc., (ISC)^2 describes many industry standards for computer security and offers the Certified Information Systems Security Professionals (CISSP) credential. The CISSP Guide distinguishes three categories of computer crime:

1. ***computer assisted crime*** – a computer is used as a tool to help carry out a crime
2. ***computer-targeted crime*** – a computer is specifically the intended victim of an attack crafted to harm the computer, network, data and its owners
3. ***computer is incidental crime*** – a computer is not necessarily the attacker nor victim, but just happened to be involved when a crime is carried out

Of note is that each of these crimes are being conducted by bad guys from every type of organization: government, military, commercial, private and criminal enterprises. When the acts are political or state-based cybercrimes, or as a part of cyberwarfare, we can note that there are international laws that seek to protect civilians during times of war. Specifically, the *Geneva Conventions*[3] apply to this situation to protect non-combatants during international armed conflict between states. Now let's look at each part of this grand protection scheme as it relates to computer and technology law to determine the 21st century evolved nature of:

- Who is a non-combatant?
- What is a conflict?
- When does a cyber-espionage and cyber-sabotage become an act of war?
- Where does a cyberattack occur?
- Why are civilian actors engaging in traditional state conflict activities?
- How can cyberattacks be considered a part of international law?

Cyberwarfare has been recognized as a significant part of armed conflict since at least the 2008 Russian conflict in Georgia (Swanson 2010). Cyberattacks on infrastructure can lead to blocked military communications, which have become of supreme necessity in managing the high technology of databases, real-time satellite remote controlled video monitored missiles, machine guns, and ballistic attacks. Control of the network of communication systems has become a necessary first step to monitoring and controlling the population, at a level whose surface was only scratched during the era of radio, newspaper and then television station control during warfare. Automated ground traffic control, air traffic and flight processes, internet commerce, and telecommunications for land-based telephone and fax are among the more mundane archaic infrastructure access and control methods.

The two prizes of cyberattacks are network control and data. The target is cyberproperty. Data is the information on the network. The tangible computer network is the hardware architecture infrastructure of satellites, telephone and cable lines, airwaves, electrical stations, communication towers, beacons, signal relays and more. Then there is software that manages, protects, and communicates data to users. Security and threats exist in both the physical and the digital aspects of the computer network. The prize sought may be access to the data, alteration of data, or access and control of the computer network. Often those legitimate and criminal parties in control of data, as intangible assets, have a great deal of power over the military and the civilian population. It is understandable how control of the civilian and municipal computer networks can greatly impair movement of the civilian population, and in a similar way control financial, social, governmental and military activity.

Network control – espionage and sabotage

Computer networks are the pipes and systems through which data flows. The "net" part is created based on an analogy to fishing nets with each cord connected to another cord to form a mesh grid of rope. Then networks evolved to mean to social groupings of people in the real world – each connected to one another directly or through links to other people and their groups

– that meet to play bridge, work on a job, study a particular subject or other social purpose. *Inter*net means a network "between" computers, linked together across various tangible and digital technologies. Then with Facebook, LinkedIn, Renren, Plaxo, Orkut, Vkontakte and others we return to the original concept as "social media networks" such that the computers linked together over the internet, telephone channels, and other means can socially interact based on interests in careers, shared hobbies, life events, and daily routines. This has at the same time established the growth of intelligence gathering jobs that monitor these social media networks and rely on GPS, cell phone tower triangulation, email and text data searches, relationship building, purchases and habits of life to predict future behavior. New jobs can be found for government contractors with titles such as "Social Media Cyber Identities Intelligence Analyst" whose quoted job description functions include:

> Analyze social networking, virtual world, and online identity issues... Manage online and virtual identity profiles… Utilize sophisticated, customized applications that collect, manage, and process online identity data… Perform appropriate methods of social network analysis to meet specific project needs. Methods may include classification, pattern analysis, trend/geo-temporal studies, and link analysis based on analysis of transaction data, message (phone, e-mail, blog) traffic, and other data sources in collaboration with other project analysts... be flexible in adapting analysis methods and different data sources to meet project needs, including willingness to learn and explore new methods/approaches.

The "explore new methods" phrase in the above job description leads me to believe that the analyst is expected to adopt "pseudo-identities" to spy on others' online behavior. This is the use of social media and intelligence gathering experts to monitor Facebook, LinkedIn, and other social networks. This monitoring is part of open source data gathering but being carried out for secret military and corporate marketing purposes by civilians. The roles played in cyber actions may originate with the same referents but are defined differently based on the particular legal, political or emotive situation. There is a clear matter of interpretation for data mining robots that crawl the web, for example, to gather, compare, and aggregate airline price fares, as this activity is termed by some as "screen scraping" but others as aggregation, depending on the legal system in place and the person conducting the activity. What has been challenged as illegal copyright infringement in the past, quickly became the search engine aggregation of the present, and this continues on to every other type of data, and then to organization, manipulation and representation of that data as it spans the network of information.

The "net" analogy has touched sciences, humanity, and crime. Transportation networks of railway, sea, and aerospace, and ground motor vehicles are intertwined via their superstructures and also their communications technologies. In recent science, the brain is described as a neuronet. Twentieth century epistemology is based on networking support for beliefs. A web, likewise, is a similar pattern of connections found by spiders in nature. Early users of the internet were called webslingers, and later, crawlers became computer programs that read websites and store data, and spiders and spyders in cyberspeak, came to mean persons or programs doing the crawling. Crimes based on criminal networks use terms such as:

- Social Engineering – Gathering information through deception of people
- Masquerading – Altering the identity's origin to appear as valid
- Emanations Capture – Intercepting electrical signals from devices; the TEMPEST standard is a defense to this threat
- Wire Tapping – Eavesdropping an electrical signal

Not far from the net, when describing a 2011 series of computer-based espionage by an undisclosed assailant, McAfee's chief European technology officer, Raj Samani, said:

> This was what we call a spear-phish attack, as opposed to a trawl, where they were targeting specific individuals within an organisation. An email would be sent to an individual with the right level of access within the system; attached to the message was a piece of malware which would then execute and open a channel to a remote website giving them access.
>
> (Emery 2011)

Criminal organizations and cybergangs are increasing using the Internet to dupe victims through false and deceitful appeals to emotion, charity and good offices along with some financial need or transaction. The net-based term used for these tricks are called "phishing attacks" and also "419 scams" and "Nigerian Letter scams." Note that analysts, contractors, criminals and bad guys use the same techniques to obtain information, but for very different ends.

Data – espionage and sabotage

The real treasure is in the data – information – secret confidential records for operating businesses, governments, and the countless details of individual lives. In accordance with the legal regime of many countries, the definition of property has been expanded to include data as property right. Courts have held that to unlawfully enter that property is a trespass. Data crimes include the unauthorized access, modification, destruction, or discloser of sensitive information. Data mining efforts can lead to information useful for the conduct of military activities, but also espionage against academic, commercial and government institutions for socioeconomic advantage and financial benefits.

Protecting intangible assets which include intellectual property, trade secrets, data, services, client lists, negotiation bids, operating expenses, air fares, and reputation can be the most difficult and the most important property for a company to protect. Consider the intellectual property, trade secrets, technology transfers, and data retrieval gold mine that can be found through your partner's computer network in a joint venture because she negligently left open their computer systems to enemies of your business.

At strategic times, data can be intercepted, altered and retransmitted sending false information and misinformation on any possible range of subject from bank accounts, to telephone transmissions, or to military targets for missile attacks. A regular series of cyberattacks was publicly reported by the famed Internet security company McAfee in August 2011, known as operation Shady RAT (Remote Access Tool) (Alperovitch 2011). The cyberattacks succeeded against 72 organizations, including defense contractors, global businesses, United Nations organizations, international organizations, government, military, university, contractor and civilian enterprises. The data retrieved, intercepted, recorded, and in some cases, altered and destroyed, has had a great effect on private civilians as well as governments. Data accessed included "U.S. military systems, the McAfee report says, as well as material from satellite communications, electronics, natural gas companies and even bid data from a Florida real estate company" (Alperovitch 2011). As operation Shady RAT demonstrated,

> A high level of access could reveal the satellite's capabilities or information, such as imagery, gained through its sensors. Opportunities may also exist to reconnoiter or compromise other terrestrial or space-based networks used by the satellite.
>
> *(Nakashima 2011)*

As described in documents of the U.S.-China Economic and Security Review Commission[4]on concerning the opportunity to control the flow of data: "The attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission." Satellite networks saturate the skies of the Earth.[5] Due to their secretive functions and relative states of decay, the exact number has become a matter of interpretation with high estimates that include many types of orbiters at around 13,000 objects. Because the data that is gathered and transmitted can only be received via specially laid out connections to other data ports in the network, satellites serve to connect data and people across the globe. In order to cover the spherical Earth at once, data relay satellites are launched into geostationary orbit, which is a location whose distance and speed enable constant communication with the Earth below to then relay information to and from other non-geostationary satellites, spacecraft, vehicles, fixed Earth stations, and personal communicator equipment. Satellites have become the pipe carrying a wealth of data through networks. Access to data via its transmitters and command-and-control infiltration is a process designed to damage and overload electrical systems, imaging equipment and data. As the 2011 USCC report describes:

> If executed successfully, such interference has the potential to pose numerous threats, particularly if achieved against satellites with more sensitive functions. For example, access to a satellite's controls could allow an attacker to damage or destroy the satellite.

One means of destroying the conduits for information flows is through strategic and conventional attacks against earth-based communication lines and systems as well as using missiles or orbiters to physically assault enemy infrastructure and satellites, this is known as the "hard attack." These hard attacks can control, interrupt or destroy energy supply systems causing power distribution outages, grid communications interruptions, and also interrupt natural energy resources for water, steam, gas and others. The "soft attack" uses digital techniques and planted misinformation to bring down the communications array and interfere with true data transmission. For infrastructure purposes, we intuitively recognize there is a need to ensure nuclear power facilities are highly protected from soft cyberattacks.

Data sharing in satellite usage becomes even more interesting when understood in light of the *Outer Space Treaties*[6] signed by all space-faring states back in 1967. They hold in relevant part that, states are prohibited from engaging in military activities in outer space and that everything that is done in outer space is the common heritage of mankind, further clarifying since the inception of the space era, that data collected in outer space is required to be shared with all of mankind. The concept is that outer space is the "Common Heritage of Humanity," also includes the principle that activities of people in outer space affect us all. From its inception, the development of space, and all of the benefits that derive from space, has been founded on the principles of equality, openness, and cooperation of all of humanity. The *Moon Treaty* (1974)[6] elaborates this, and it is held that everything discovered, invented, created, destroyed, explored, defined, developed, and so on, in outer space will gradually trickle down and reach all people everywhere. As such, the activities carried out in outer space, the right to conduct such activities, and the benefits from those activities belong to our “World Heritage.” Travelers (astronauts and tourists) to outer space are not merely state government passengers but treaty designated “envoys of mankind” and according to the agreements of all the states that signed the treaties, we all have a right to access of the data acquired by these envoys (*The Outer Space Treaty of 1967*, Article 5). The issues of satellite and mobile phone data is precisely the technology intended to be guided by the outer space principles as these satellite-based technologies have clearly affected all of mankind. Therefore, the use of secretive government and military applications for cell phone data may be seen as contrary to treaty obliged openness and non-militaristic uses for outer space, and the international legal regime that enabled the peaceful development of outer space that we presently enjoy.

A relevant example is found in the use of remote imaging satellites to gather data about the Earth via satellite imagery. According to the law of the *Outer Space Treaties*, remote sensing data can be used to benefit all of humanity. Remote sensing imaging machines and applications measure, map, image, track and observe all manner of phenomenon on Earth and in outer space. Sustainable development resources can be allocated and business plans can be made based on data about vegetation rates, erosion, pollution, forestry, weather, and land use. City planning, archaeological investigations, military observation and geomorphological surveying also are enhanced based on remote sensing data. Remote sensing data is more than just nice pictures or nuclear missile detection spy satellites, as the data tells us about how to prospect for minerals, detect or monitor land usage, understand deforestation, and examine the health of indigenous plants and crops, and how to farm entire regions or forests. Landsat-7 is designed to take up to 582 high-resolution images of the Earth's terrain each day, and in accordance with the *Outer Space Treaties*, these images are publicly distributed, such that private companies like Google Maps, may color-balance and enhanced them for commercial services. So it is telling that the cyberattacks of 2012 against officially non-military satellites, in this case the U.S. Geological Survey satellite Landsat-7, are described as contrary to space law’s peaceful cooperation principles, and even international humanitarian law’s protection of civilian structures from military targeting. As the satellite was used for peaceful purposes, with data benefits that are shared for the common heritage of all mankind, the attack on this network harmed us all. As a matter of international space law, regardless of the individual, criminal organization, government or military affiliation of the bad guy, her activities directed toward outer space fall under the liability of the state of origin of those activities, i.e., the launching state (*The Outer Space Treaty of 1967*, Article 7).

State and non-state Actors migrate from the war on terror to cyberwar

There is a long tradition of government contractors to support military services. Outsourcing is much cheaper for the government in terms of retirement, pension, healthcare and other benefits, and for their works, they receive higher salaries as a private contractor than as a government employee. But is the job being done for state purposes or military purposes – when the duties have traditionally been part of a military job, or a government job, now being contracted out to a civilian? Does the data gathering, retention, security, or theft of this data fall into the realm of the government public international law or private company liability? The basic rule applicable from International Humanitarian Law (IHL)[7] is to protect civilians during armed conflict.

State actors traditionally include government officials, the, police and the military. Non-state actors are civilians, independent contractors, cybergangs and terrorists. Whatever the parties' affiliation, international law remains the law between states. The basic rule of distinction is that parties to conflict are required to at all times distinguish between civilians and combatants, and then their attacks are required to be directed solely against military objectives. This principle requires combatants to only attack military objectives and not the civilian population, nor individual civilians, nor civilian property including hospitals, schools, religious buildings, historical and cultural structures, nor industrial infrastructure used for civilian purposes.[8]

Let's consider the status of civilian contractors performing highly specialized work that has traditionally been carried out by the governments to develop, monitor, and implement data gathering programs. In every country, especially the USA, Russia, China, and throughout the EU, following the post 9-11 changes that have led to highly developed security regimes, there has also developed a remarkable increase in private entities that own infrastructures that are critical to national security interests. Use of private company equipment, vehicles and personnel for support of military activities confuses the civilian/military distinction. Here we recognize the traditional construction workers, war machine factory employees, food preparation and delivery enterprises that are contractors for the military, and for Law of War purposes, are considered civilians that accompany the military. But recent developments also include having private civilian security services to guard buildings, install technology wiring, computers, networks, and video and communications equipment. Also now, we have delivery of space satellites on privately launched vehicles, and development of surveillance equipment for audio, video, purchases, movement, lifestyle and choice of life data. Is this military data or civilian data? Is this data used to observe threats to national security or for military uses or for corporate marketing campaigns? In a legal sense, does the military enter into the domestic civilian police force during the conduct of surveillance cyberattacks, data theft, and network control?

The civilians' role has evolved in part as a reaction to decreased government spending for traditional military types of work. Defining civilians and their role in the relationships between government-military-university-private contractors has become complex. The traditional rule is that civilians are not part of the military.[9] Furthermore, the traditional rule holds, civilians are non-combatants and are not engaged in conducting acts of aggression. Increasingly, civilian government contractors are in control of more technology for remote surveillance, data capture, and increasingly employ more techniques to disrupt and control the electronic equipment of other enemies.

At other times these remote attacks take the form of drone strikes carried out against non-military persons, civilians and terrorists, and these attacks are based on data produced, gathered analyzed and reported by non-government employees, i.e., contractors. The "civilian" status becomes particularly relevant when the information gathering "unmanned aerial vehicle" mounts a weapon and becomes a remote controlled attack drone; or even as an autonomous robotic weapon system that fully automates in a self-contained and independent manner once deployed to a kill zone. When the machine is designed and deployed by civilians, and persons killed are civilians, it becomes difficult to determine who are the combatants in this state sponsored act, in zone that may or may not be declared a war zone.

Suppose a state party decides to destroy a government contractor surveillance institution operating remotely because the attacking government believes the civilian contractors are conducting cyber espionage, sabotage, as well as, property taking of confidential records for socioeconomic advantage, or destruction of civilian tangible assets and intangible assets from that site. From IHL,[7] three rules apply to military actors, and it remains to be determined at what point the remote cyber surveillance civilian actor becomes a combatant:

1. An indiscriminate attack occurs when the military fails to make this civilian, combatant and non-combatant distinction in its activities. This is the essence of a war crime.
2. Combatants must always take precautions to minimize causing harm to non-combatants.
3. Excessive attacks are ones that are likely to cause death or injury to civilians or are attacks that are likely to damage non-military civilian objects. Proportionality is

> required in military decision making to minimize harm to civilians while carrying out military objectives.

The linguistic evolution of “war” to “armed conflict” to the “war on terror” and now to “cyberwar” has coincided with the evolution of the meaning of attack, criminal, and belligerent. As noted by FBI Director Robert Mueller who testified that cyber threats will surpass terrorism as the top threat facing the United States. “Stopping terrorists is the number one priority,” stated Mueller, “But down the road, the cyber threat will be the number one threat to the country. I do not think today it is necessarily [the] number one threat, but it will be tomorrow” (Hoover 2012).

Cyberwar and cyberattacks come from all types of bad guys. The laws of armed conflict are ambiguous as to whether members of armed opposition groups are considered members of armed forces or civilians, so for our purposes cybergang status is likewise ambiguous but is merely another type of bad guy conducting attacks to control communications networks, data, and financial and military weapons. So the cyberwar is against all manner of bad guys – states, cybergangs, enemy military, and hackers.

So let’s now briefly consider the meaning of this “state of war.” Traditionally, a declaration of war is an announced position for acts of hostility by one state party against another state party. The legality of who in the government is competent to declare war varies based on the country, but in the USA, it is the Congress that has the Constitutional authority to declare that the USA is in a war with another country. This declaration power has not been used by the USA since it last declared itself to be in a war in 1942. “Armed conflict” is a concept that has evolved as a counter to the need for a declaration of war and is based on the fact that the nature of military actions has changed away from states’ declarations. In many modern states today, this warlike aggression is now titled “authorization to use military force.” Rather than be concerned with the politics and rhetoric of states regarding whether a particular conflict is a war or not, international law applies for armed conflict as defined as “any use of armed force by one State against the territory of another,” so that it triggers the applicability of the Geneva Conventions between the two states (Gasser 1993). According to this scheme, measures taken to prevent cyberwarfare and the carrying out of attacks during cyberwarfare would be governed by the same legal regimes that other types of “armed conflict.”

Surveillance and border security

The meaning of a technology crime or attack depends largely upon the definition of the parties involved. Police use of magnetic GPS radio transmitters secretly attached to a car, without obtaining a warrant from a judge, might be seen as legal. But if instead of the police the same activity is conducted by a jealous ex-husband, or a business competitor, or an advertising company seeking to learn market strategies for its goods, or to monitor an employee's private vehicle that she drives in part for performance of work related duties – then the culpability of the act becomes more certain. Cyberlaw, and international cyberwarfare, must consider the limits of government and corporate penetration into private civil life.

The meaning of borders has changed. We once lived in a world with less immigration, passport and border security controls. As globalization and ease of mass transportation has greatly increased, the nature of border security has evolved such that it becomes more and more difficult for legal entry into another country. Illegal entry immigration remains a fact of everyday life in every country. The distinction between resident and migrant becomes linguistically and legally blurred. The meaning connected to this legal glossary has changed greatly in the past two decades, resulting in the marginalization of certain groups, in effect defining their legal status out of existence, and simultaneously empowering other groups with new authoritative meaning, identity, power, representation, and jurisdiction.

Some argue that this is a situation that many governments seek to maintain, because so much of their domestic economy depends on the labor of "undocumented" workers. Terms such as "without status" "migrant," and "illegal immigrant" have become legally fashionable. In the USA, contract managers can hire these laborers from "south of the border" by scouting them out from groups of men waiting for drive-by pickup trucks to hire them to do the most menial and physically demanding of jobs. Of note here is the convenient legal linguistic situation of the "contractor." The owner of the construction project or factory or business is not the employer of the laborers. In practice, the project is run by a principal who hires contractors for specific parts of the job: the laborers are hired by the "independent contractor" so that any legalities or illegalities in work performance or standards are buffered to the liability of this very independent contractor, thereby immunizing the ultimate owner of the business or construction project. This independent contractor situation protects the principal from all sorts of immigration, healthcare, housing, food, working hours, environmental standards, machinery and equipment safety requirements. Another byproduct of this undocumented labor is the denial of taxes and community contributions greatly needed by the governments during the worst of economic times, yet unpaid by "workers without status." In Northern California it has been reported that the average life expectancy of illegal migrant farm worker is "still 49 years -- compared to 73 years for the average American."[10] There are parallel situations in every country.

So while airport security does full nude image body scans, diary readings and on-sight translations, along with total computer, cell phone and digital camera harddrive data copying and weeklong computer seizures – workers without status in well-known districts remain in every major world city, out in public to be hired as servants to work without rights. Similar criminal networks develop for the sex industry, as much of its labor comes from mass and secretive movement and abduction of women, girls, and boys trapped in this undocumented underground economy. Many live and die secretly in the same country for 80 years or are even born in that country, but never attain citizenship rights or even residency permission, despite massive amounts of electronic data collected about them. The government is concerned with who is the tourist, businessman, and resident, as well as, who is the potential terrorist. The result is that the level of publicly-displayed high technology surveillance and adherence to the immigration tracking rules is at a worldwide all-time high, yet it is difficult to reconcile this level of scrutiny with the number of unprotected and undocumented travelers and laborers.

Conclusion

The technology to record, monitor and influence human movement and activities is highly sophisticated. There are many parties leading the social and legal movement to involve computers in all aspects of government affairs, financial endeavors, political activism, travel, migration, and criminal behavior. But there are common security threads legally found throughout international law, computer law, and the law of armed conflict that prove to have application to the cybercrimes and cyberwars of the newest era.

References

Alperovitch, D. (2011, Aug). Revealed: Operation Shady RAT. McAfee White Paper. http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf

Draetta, U. (2005). *The Internet and electronic commerce in international business law*. The Hague Academy of International Law.

Emery, D. (201, Aug 3). Governments, IOC and UN hit by massive cyber attack. *BBC News*.

Gasser, H.P. (1993). International humanitarian law: An introduction. In H. Haupt (Ed.), *Humanity for All: The International Red Cross and Red Crescent Movement*, p. 510-511. Berne: Paul Haupt Publishers. http://www.bbc.co.uk/news/technology-14387559

Hoover, N. J., (2012, Feb 1). Cyber attacks becoming top terror threat, FBI says. *InformationWeek*. www.informationweek.com/news/government/security/232600046

Nakashima, E. (2011, Aug 3). Report on 'Operation Shady RAT' identifies widespread cyber-spying. *Washington Post*. https://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html

Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. *Loyola LA International and Comparative Law Review 32*(2) 303-333. http://digitalcommons.lmu.edu/ilr/vol32/iss2/5

Online References

Outer Space Treaty of 1967 https://history.nasa.gov/1967treaty.html

Moon and other Celestial Bodies Moscow, London & Washington, January 27, 1967 https://www.state.gov/wp-content/uploads/2019/05/225-Outer-Space-Treaty-website-1.pdf

Rescue Agreement 1968 https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html

Liability Convention 1972 https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html

Registration Convention 1974 https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html

Moon Agreement 1974 https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/travaux-preparatoires/moon-agreement.html

End Notes

1. Separate papers written by the author regarding cybersecurity describe legal aspects of intellectual property, trade secrets, technology, transfers, satellite, data retrieval, travel law, and international humanitarian law.
2. This training is offered by many organizations including, e.g., the EC-Council which "provides a comprehensive ethical hacking and network security-training program to meet the standards of highly skilled security professionals." An archived copy of the CE Council page may be found at https://web.archive.org/web/20120325073617/www.eccouncil.org/courses/certified_ethical_hacker.aspx
3. *The Geneva Conventions* comprise four treaties, and three additional protocols, that establish the standards of international law for the humanitarian treatment of the

victims of war. The treaties text and International Committee of the Red Cross (ICRC) commentary can be found at https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/

4. The U.S.-China Economic and Security Review Commission (USCC) https://www.uscc.gov/ *2011 Annual Report*, and described by Mick, Jason DailyTech, *Gov't Report Warns of Chinese Plans to Cripple U.S. Space Defenses,* November 17, 2011. Archive copy at https://archive.li/xTKEj
5. The real time locations of 13,000 of these satellites can be seen on via the official KML file https://www.gearthblog.com/satellites or via the Google Earth Plug-in.
6. *Treaty Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies* Moscow, London & Washington, January 27, 1967. Et seq. Five Outer Space Treaties – *Outer Space Treaty* 1967, *Rescue Agreement* 1968, *Liability Convention* 1972, *Registration Convention* 1974, *Moon Agreement* 1974.
7. International Humanitarian Law (IHL) to also include Geneva Conventions, the Hague Conventions, Law of War and Armed Conflict (LOW and LOAC), human rights law, war crimes, and proceedings of International Criminal Court (ICC).
8. A useful collection of customary rules of IHL are summarized and organized on the International Committee of the Red Cross (ICRC) website at https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul
9. The Geneva Conventions define civilian status and the civilian population. The definition of civilians is as persons who are not members of the armed forces. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1) Chapter II: "Civilians and Civilian Population", Article 50 to which no reservations have been made, and virtually all states agree. This custom and standard is also restated in numerous military manuals and military practice. The International Criminal Tribunal for the Former Yugoslavia adjudicated the Blaškić case in 2000, defining civilians as "persons who are not, or no longer, members of the armed forces."
10. The Cesar E. Chavez Foundation and the United Farmworkers of America. https://ufw.org/