THE COLLAPSE OF UN TALKS ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE: WHY IT MATTERS TO U.S. BUSINESSES

Date: 24 May 2018

U.S. Insurance Coverage / Cyber Law and Cybersecurity Alert

By: Lucas J. Tanglen, Reymond E. Yammine

It is commonly said that cyberspace is the “Wild West,” a realm where there are no laws and no sheriff in sight. Even acknowledging that this view contains a degree of hyperbole, it is unfortunately no less true after last year's fruitless conclusion to a decade's worth of international discussions regarding the future of international law in cyberspace. [1] The United Nations (“UN”) Group of Governmental Experts (“GGE”) on Developments in the Field of Information and Telecommunications in the Context of International Security had been considering the application of international norms to the member countries' activities in cyberspace. Traditional powers, including the United States, China, and Russia, had participated in the effort, [2] but negotiations were ultimately frustrated, as divisions along old “Cold War” lines prevented agreement on key terms. [3] In light of this development, cyberspace appears likely to remain an international “Wild West,” with no established legal framework to address cyber attacks carried out or otherwise supported by nation-states.

This is important to U.S. companies because recent history — including the indictment last month of nine Iranian nationals in a “massive cyber theft” and 2017's WannaCry and NotPetya destructionware attacks, which have been attributed to North Korea and Russia, respectively — shows that attacks by nation-states, even when they are not directed at U.S. businesses, may have substantial adverse effects on those companies. Accordingly, U.S. companies need to understand their potential vulnerability to nation-state cyber attacks and the possibility of using their insurance to manage those risks. [4] This article explores the development and ultimate collapse of the UN cyber talks, the implications for U.S. businesses, and insurance considerations in light of the ongoing threats.

THE UN TALKS ON INTERNATIONAL NORMS FOR CYBERSPACE

In 1999, the UN General Assembly recognized the “scientific and technological” value that cyberspace represented and the need to protect its civilian uses. [5] The General Assembly concluded that it was “necessary to prevent the misuse or exploitation of information resources” and that member states should work toward considering the “[a]dvisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.” [6] The GGE officially began its work in 2004 and, over the years, seemed to make advancements toward an international legal framework.

The GGE recognized the impact that the development of information and communications technologies (“ICTs”) could have on matters of national security. In 2009, the group alerted states that the growing use of ICTs would

©2005-2021 K&L Gates LLP. All Rights Reserved.

create “new vulnerabilities and opportunities for disruption.” [7] Indeed, the GGE pointed out that “the same technologies that support robust e-commerce can also be used to threaten international peace and national security.” [8] The GGE recommended, among other things:

- Increasing dialogue among states to discuss norms concerning ICTs, in order to protect critical national and international infrastructure;
- Creating information exchanges regarding national ICT legislation; and
- Identifying measures to support capacity building in less-developed countries. [9]

In 2013, the GGE acknowledged the importance of maintaining an international legal framework that could preserve peace in cyberspace. The group's recommendations stated, “the application of norms derived from existing international law . . . is essential to reduce risks to international peace, security and stability.” [10] Furthermore, “States must not use proxies to commit internationally wrongful acts” and should seek to ensure “that their territories are not used by non-State actors for unlawful use of ICTs.” [11]

In 2015, the GGE noted “[t]he diversity of malicious non-State actors, including criminal groups,” which could create misperception of state action and the “possibility of harm to their citizens, property and economy.” [12] The GGE called again for increased cooperation between nations and the use of ICTs in a way consistent with preserving “global connectivity and the free and secure flow of information.” [13]

Despite such indications of progress, 2017 brought the breakdown of the GGE's talks. The failure of the negotiations was ultimately driven, in part, by what media described as divisions along Cold War lines. [14] On one side, U.S. expert to the GGE, Michele Markoff, argued that the GGE was misguided in not seriously considering the inclusion of the member states' right to self-defense against foreign-state attacks. [15] The right to self-defense, in its broad sense and as memorialized in Article 51 of the UN Charter, refers to a state's right to respond to an “armed attack” against it. [16] Markoff argued that the recognition of the right to self-defense in the cyber context would “help reduce the risk of conflict by creating stable expectations of how states may and may not respond to cyber incidents they face.” [17] On the other side, Cuba opposed recognizing a right to self-defense, arguing that such a regime would “convert cyberspace into a theater of military operations and . . . legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs.” [18] Having reached an impasse, the GGE officially dissolved in 2017. [19]

FOREIGN-GOVERNMENT CYBER ATTACKS ARE LIKELY TO HIT U.S. BUSINESSES

The practical implications of the failure of the GGE talks come into greater focus against the backdrop of near-daily news of globally significant cyber incidents. Contrary to a previously popular depiction of hackers as rogue, individual actors, governments and experts have come to understand that many cyber attacks, including those targeting businesses, are carried out or supported by foreign governments.

For example, in March 2018, the Department of Justice announced charges against nine Iranian nationals for their alleged participation in a massive cyber theft affecting 30 U.S. companies, five governmental agencies, and 176 universities across the globe. [20] Deputy Attorney General Rod J. Rosenstein stated that these individuals

©2005-2021 K&L Gates LLP. All Rights Reserved.

"acted at the behest of the Iranian government, and specifically, the Iranian Revolutionary Guard Corps." [21] The Iranian Revolutionary Guard Corps, better known as the Islamic Revolutionary Guard Corps, is classified as a terrorist organization by the Department of Treasury for providing assistance to the Iranian military and for its involvement in the Syrian civil war. [22]

Similarly, two recent "ransomware" attacks, which in fact only masqueraded as ransomware attacks but were actually destructionware attacks — WannaCry and NotPetya — have been attributed to foreign governments by the United States. These two attacks illustrate the disruption and enormous costs that nation-state cyber attacks can inflict on businesses. Starting in March 2017, WannaCry — which the United States (and United Kingdom) have attributed to North Korea [23] — wreaked havoc in many parts of the business world by virtually holding hostage hundreds of thousands of computers. [24] WannaCry crossed international borders, hitting businesses across many industries, [25] including banks, car manufacturers, and hospitals. [26] Then, in June 2017, NotPetya — which the United States has attributed to Russia [27] — brought another wave of cyber-chaos across borders and industries. [28] Some sources estimate that these attacks caused almost $5 billion in global financial losses. [29] Importantly, neither of these attacks specifically targeted U.S. companies, but they nevertheless quickly crossed borders through cyberspace, resulting in widespread damage to U.S. companies.

Of course, the threat of nation-state cyberattacks against businesses and other entities is not limited to ransomware schemes. Several other high-profile cyber attacks have been attributed to governments, including:

- Stuxnet, the computer worm that in 2011 attacked and effectively halted Iran's nuclear program. The worm was widely attributed by the media to a joint American and Israeli effort. [30]
- The 2016 cyber theft of $81 million of Bangladeshi funds from the New York Federal Reserve, which has been attributed by the media to North Korea. [31]
- The hacking of the Democratic National Committee's servers in 2016, which U.S. investigators suspect was supported by the Russian government, [32] and the February 2018 indictment by the Special Counsel's Office of 13 Russian individuals for their alleged involvement in online "information warfare" related to the 2016 election. [33]
- The hacking of HBO in May of 2017, which led to a $6 million extortion scheme against HBO and a leak of "Game of Thrones," attributed by the Department of Justice to an Iranian national who had previously assisted the Iranian military in their cyber attacks. [34]
- The attack on Ukraine's electrical grid in December of 2015, which caused more than 200,000 consumers to lose power and has been attributed by the media to Russian groups. [35]
- The attack on Saudi Arabia's state oil company in 2012 through the use of "Shamoon," a virus designed to wipe target hard drives clean of data. [36] The U.S. Department of Homeland Security attributed the attack to Iran. [37]
- The cyber attack against the World Anti-Doping Agency ("WADA") in the summer of 2016, causing the leak of athletes' confidential medical data, which WADA attributed to a Russian cyber-espionage unit named "Fancy Bear." [38]

©2005-2021 K&L Gates LLP. All Rights Reserved.

- The alleged cyber espionage against several major U.S. companies by members of the People's Liberation Army of China between 2006 and 2014, which resulted in federal indictments of five alleged Chinese military hackers. [39]
- A series of cyberattacks in 2012 and 2013 against several U.S. financial institutions, which disrupted operations through the use of Denial-of-Service attacks. [40] The U.S. Department of Justice attributed these attacks to a group of Iranian individuals acting on behalf of the Iranian Revolutionary Guard Corps. [41]

A clear lesson from these examples is that nation-state cyberattacks represent a serious risk to all businesses and organizations that do business in cyberspace. Indeed, the Council of Economic Advisers warns that nation-states may attack businesses "potentially as a retaliation against sanctions or other actions taken by the international community." [42] Many cyber incidents cannot properly be understood like some "traditional" risks — for example, the sinking of a ship or a fire in a factory — which might be viewed as one-off events that affect a particular business in a particular industry. Rather, nation-state cyberattacks frequently cast an extremely wide net, and a single attack might spread to affect hundreds of organizations or more while it runs its course over a period of weeks or months. Particularly given the failure of the UN GGE discussions, there is every reason to expect that nation-states might continue or expand their use of cyberspace to pursue their geopolitical goals. As the President's National Infrastructure Advisory Council stated in a draft report: "Cyber is the sole arena where private companies are the front line of defense in a nation-state attack on U.S. infrastructure." [43]

MAGNITUDE OF THE RISK AND SOME INSURANCE CONSIDERATIONS

The potential losses associated with a cyberattack include, but are not limited to, stolen or corrupted data; business interruption and extra expense losses; damage to reputation and brand; and various response costs in the form of fees for forensic investigators, notification of affected consumers or vendors, and establishment of call centers and credit monitoring. Indeed, it is the ability of a cyber attack to significantly disrupt vital processes that may make international cyberattacks an appealing option for nation-states. [44]

Given the immense threat posed by international cyber attacks and the apparent failure of the international community to develop a legal framework to deter nation-state cyber attacks, there is no time like the present for policyholders to understand potential insurance coverage for this type of risk. "Traditional" insurance may provide coverage for certain Internet-related losses and liabilities. Such "traditional" coverages include commercial property policies, commercial general liability insurance, and errors and omissions (or professional liability) insurance policies. Policyholders will want to review carefully whether any "cyber" exclusions that may limit or divest the policyholder of coverage have been included in those policies. Depending on policy wordings, insurers may assert that certain cyber risks are not covered by such "traditional" insurance.

In recent years, the number and variety of specialty cyber-insurance coverages has grown significantly, with approximately 70 insurers currently offering some form of cyber coverage. Cyber policies may differ widely in the types of coverages provided and the scope of coverage that would be provided in the event of a cyber attack.

Because of the nature of these attacks, business interruption coverages are likely to be implicated. With cyber attacks like WannaCry and NotPetya, a victim's entire computer network may become unusable for a period of time. Such downtime may translate into significant costs, including lost profits and the extra expenses of

©2005-2021 K&L Gates LLP. All Rights Reserved.

mitigating such losses. Policyholders may wish to consider whether their current policy contains coverage for business interruption and whether there are any relevant policy exclusions for attacks allegedly or actually initiated by nation-states.

For example, some insurance policies contain exclusions related to “war,” “warlike action,” “terrorism,” “hostilities,” and “hostile acts,” which an insurer might invoke in an attempt to avoid coverage. Policyholders should not assume that such an exclusion necessarily bars coverage for a particular cyberattack. The precise wording of each exclusion, which may vary substantially among policies issued by different insurers, should be applied carefully and narrowly. For example, depending on the wording of the exclusion, it may be very difficult for an insurer to establish that a particular cyber attack rises to the level of, for example, “war” or “warlike action.” Similarly, the undefined term “hostilities” (for example) is very vague and ambiguous. Where an ambiguous term like “hostilities” appears in a list with other excluded events such as “war” and “warlike action,” the doctrine of ejusdem generis holds that the meaning of the ambiguous term should be restricted to something similar to “war” or “warlike action.” Also, the origin of a cyber attack is often unclear and subject to dispute, even years after the attack occurred. It may be inappropriate for an insurer (who generally bears the burden of proving that an exclusion applies) to invoke an exclusion where there exists any uncertainty as to a cyber attack's origin, even if government or media sources have attributed the attack to a government or military entity.

Most cyber policies also contain exclusions for property damage and bodily injury. Cyber-physical attacks are real, and are no longer just the product of speculation. For example, a cyber attack may affect monitoring software meant to keep processes under control, like electronic gauges, GPS systems utilized in transportation environments, and even vital cooling systems for valuable computer networks. A careful analysis of how property damage and bodily injury exclusions might apply may be very useful in assessing the responsiveness of a cyber policy to such a cyber-physical attack.

As the foregoing suggests, it is in a policyholder's interest to carefully review, in consultation with insurance coverage counsel, the wording of any cyber insurance that the company currently has in effect or is considering purchasing. Policyholders and their counsel may be able to negotiate with insurers during the placement or renewal of an insurance program to obtain more favorable wording than the “off-the-shelf” language might provide (including with respect to “war” exclusions and other exclusions).

Likewise, in the event that an organization finds itself in the unfortunate position of being a victim of a cyber attack, coverage counsel can assist with a prompt, careful review of any potentially applicable insurance policies and analyze the necessary steps to pursuing potential insurance coverage (including the timely provision of notice to relevant insurers).

---

[1] *See* Michele Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.S. MISSION TO THE U.N. (June 23, 2017) (the “Markoff Remarks”), https://usun.state.gov/remarks/7880.

[2] *See, e.g.*, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/65/201, at 5, (July 30, 2010) (the “2010 GGE Report”).

©2005-2021 K&L Gates LLP. All Rights Reserved.

[3] *See* Owen Bowcott, *Dispute along cold war lines led to collapse of UN cyberwarfare talks*, THE GUARDIAN (Aug. 23, 2017), https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges.

[4] Indeed, the Council of Economic Advisers estimates that cyberattacks cost the U.S. economy "between $57 billion and $109 billion in 2016." *The Cost of Malicious Cyber Activity to the U.S. Economy*, WHITE HOUSE (February 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf at 2. One source estimated that the average cost to a U.S. business is about $21 million per attack. *See Cyber Crime Costs $11.7 Million Per Business Annually*, SECURITY MAGAZINE (Sept. 26, 2017), https://www.securitymagazine.com/articles/88338-cyber-crime-costs-117-million-per-business-annually.

[5] G.A. Res. 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security (Jan. 4, 1999).

[6] *Id.*

[7] 2010 GGE Report, U.N. Doc. A/65/201, at 2.

[8] *Id.*

[9] *Id.* at 8.

[10] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 2, U.N. Doc. A/68/98 (June 24, 2013).

[11] *Id.* at 8.

[12] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 6, U.N. Doc. A/70/174 (July 22, 2015).

[13] *Id.* at 13.

[14] *See* Bowcott, *supra* note 3.

[15] *See* Markoff Remarks.

[16] *See* U.N. Charter art. 51.

[17] *See* Markoff Remarks.

[18] Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017), http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

[19] *See* Bowcott, *supra* note 3.

[20] *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Revolutionary Guard Corps*, DEP'T OF JUST. (Mar. 23, 2018), https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

[21] *Id.*

©2005-2021 K&L Gates LLP. All Rights Reserved.

[22] *Treasury Designates the IRGC under Terrorism Authority and Targets IRGC and Military Supporters under Counter-Proliferation Authority,* DEP'T OF TREASURY (Oct. 13, 2017), https://www.treasury.gov/press-center/press-releases/Pages/sm0177.aspx.

[23] *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, WHITE HOUSE (Dec. 19, 2017), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917; *Britain believes North Korea was behind "WannaCry" NHS cyber attack*, REUTERS (Oct. 27, 2017), https://www.reuters.com/article/us-britain-security-northkorea/britain-believes-north-korea-was-behind-wannacry-nhs-cyber-attack-idUSKBN1CW153.

[24] Nicole Perlroth, *More Evidence Points to North Korea in Ransomware Attack*, N.Y. TIMES (May 22, 2017), https://www.nytimes.com/2017/05/22/technology/north-korea-ransomware-attack.html.

[25] Sheera Frenkel, *Global Ransomware Attack: What We Know and Don't Know*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/global-ransomware-hack-what-we-know-and-dont-know.html.

[26] *See* Elizabeth Dwoskin & Karla Adam, *More than 150 countries affected by massive cyberattack, Europol says*, WASH. POST (May 14, 2017), https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.2f6f1a3871fb; *see also* Jackie Wattles, *Who got hurt by the ransomware attack*, CNN (May 14, 2017), http://money.cnn.com/2017/05/13/technology/ransomware-attack-who-got-hurt/index.html.

[27] *Statement from the Press Secretary*, WHITE HOUSE (Feb. 15, 2018), https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

[28] Ellen Nakashima, *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.82b5ce3925b4.

[29] WannaCry is estimated to have caused approximately $4 billion in losses, while NotPetya is estimated to have caused around $850 million in losses. Jonathan Berr, *"WannaCry" ransomware attack losses could reach $4 billion*, CBS NEWS (May 16, 2017), https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/; Jim Finkle, *Cyber 'worm' attack hits global corporate earnings*, REUTERS (Aug. 2, 2017), https://www.reuters.com/article/cyber-results/cyber-worm-attack-hits-global-corporate-earnings-idUSL1N1KO0VB.

[30] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?rref=collection%2Ftimestopic%2FStuxnet.

[31] Edvard Pettersson & Tom Schoenberg, *North Korea Link Probed in $81 Million Theft of Fed Funds: Sources*, BLOOMBERG (Mar. 22, 2017), https://www.bloomberg.com/news/articles/2017-03-22/north-korea-link-said-to-be-probed-in-n-y-fed-account-theft.

[32] *See Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE (Jan. 6, 2017), http://www.dni.gov/files/documents/ICA_2017_01.pdf, at ii; *see also* Eric Lipton, David E. Sanger & Scott Shane,

©2005-2021 K&L Gates LLP. All Rights Reserved.

The Perfect Weapon: How Russian Cyberpower Invaded the U.S., N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[33] *Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System*, DEP'T OF JUST. (Feb. 16, 2018), https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[34] *Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO*, DEP'T OF JUST. (Nov. 21, 2017), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting.

[35] Donghui Park, Julia Summers & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, U. OF WASH. (Oct. 11, 2017), https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[36] *Saudi Arabia warns on cyber defense as Shamoon resurfaces*, REUTERS (Jan. 23, 2017), https://www.reuters.com/article/us-saudi-cyber/saudi-arabia-warns-on-cyber-defense-as-shamoon-resurfaces-idUSKBN1571ZR.

[37] *Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017*, WHITE HOUSE (June 26, 2017), https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/.

[38] *WADA Confirms Attack by Russian Cyber Espionage Group*, WADA (Sept. 13, 2016), https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group.

[39] *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, DEP'T OF JUST. (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[40] Denial-of-Service attacks rely on overloading a target network's capabilities by sending high loads of traffic far exceeding the target's capacity.

[41] *United States v. Fathi, Indictment*, DEP'T OF JUST., https://www.justice.gov/opa/file/834996/download.

[42] *The Cost of Malicious Cyber Activity to the U.S. Economy*, WHITE HOUSE (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, at 3.

[43] *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, DEP'T OF HOMELAND SEC. (August 2017), https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

[44] *Id.* at 5.

©2005-2021 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS

LUCAS J. TANGLEN
PARTNER

PITTSBURGH
+1.412.355.7479
LUCAS.TANGLEN@KLGATES.COM

REYMOND E. YAMMINE
ASSOCIATE

NEWARK
+1.973.848.4127
REYMOND.YAMMINE@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2021 K&L Gates LLP. All Rights Reserved.