THE TIMES OF ISRAEL | www.timesofisrael.com
This post has been contributed by a third party. The opinions, facts and any media content here are presented solely by the author, and The Times of Israel assumes no responsibility for them. In case of abuse, report this post.

US vs. Russia: A watershed moment in cyberspace and cyber-diplomacy

DEBORAH HOUSEN-COURIEL | DECEMBER 30, 2016, 2:47 PM |

In an intriguing and significant development in the deepening confusion around what's permitted and forbidden to states in cyberspace, the White House yesterday issued sanctions against Russia via Executive Order 13694, ominously entitled "Taking Additional Steps to Address the National Emergency with respect to Significant Malicious Cyber-Enabled Activities." The Order is being called the most severe imposition of US sanctions on Russia since the end of the Cold War.

In addition to the sanctions, which are imposed upon several Russian officials and security agencies such as the GRU and FSB, the State Department has expelled 35 Russian diplomatic representatives and their families from US territory, declaring them "persona non grata." The aim of the Order is to isolate these individuals and organizations, curtailing their financial freedom of activity outside of Russia, and to send a clear message to Russia and other unfriendly actors in cyberspace that hostile cyber activities against the US and its democratic institutions – in particular, its electoral process — are unacceptable and will incur international repercussions. In turn, Russia has already publicly responded, vowing a 'proportional response."

This is not the first instance of the US imposing sanctions on another state in response to hostile actions in cyberspace. North Korea was similarly sanctioned in 2015, in the wake of that country's alleged infiltration and leakage of Sony Pictures databases in anticipation and protest of the release of Sony's movie "The Interview," mocking North Korean leader Kim Jong-un. Likewise, in 2014 the Justice Department indicted five Chinese citizens, members of the People's Liberation Army, on hacking charges, and in the following year threatened trade sanctions against China for that country's alleged economic espionage. Yet the latest Executive Order adds financial sanctions relating specifically to a new phenomenon in cyberspace, the alleged Russian intervention in recent US national elections.

The Order itself declares a state of national emergency, effective immediately, "…with respect to significant malicious cyber-enabled activities…and in view of the increasing use of such activities to undermine democratic processes or institutions." It comes as part of the promised US response to hostile Russian interference in the US presidential campaign and electoral process, widely covered and discussed in the media in recent weeks. The data breaches into the Democratic National Party's databases and the subsequent exposures by Wikileaks,

fabricated news articles, and exploitation of social media are some of the hostile activities allegedly initiated by Russia or Russian agents and “trolls.”

President Obama had stated that the US government would respond to cyber-enabled meddling with US elections with both overt and covert measures, and asked for a full investigation of such activities and their technical attribution. In the fall of 2016, and continuing up until the past few weeks, the FBI, Department of Homeland Security and other agencies, which dubbed the operations “Grizzly Steppe,” supplied the requisite evidence attributing to Russia.

The sanctions imposed by the Order include freezing the transfer of assets and property located in the United States of persons who are responsible for or complicit in cyber-enabled activities originating outside the US that are reasonably likely to result in a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. Not only those actually orchestrating these activities are subject to the freezing of financial property located in the US, but also those the hackers who carried out the cyber disruptions and anyone who funded or otherwise materially assisted such efforts. Hundreds, if not thousands of people are implicated, given the number of cyber interventions and the extended time period over which they occurred.

In practical terms, the list of hostile cyber activities subject to the imposition of sanctions is lengthy. It includes cyber disruptions that adversely affect critical infrastructure, such as electrical grids and water systems; intrusions into computer networks; and misappropriation of economic resources, trade secrets, and financial and personal data for commercial or competitive gain. Yet these are all general background to the real motivation for the Order, section E of which specifies the prohibited acts of “…tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.”

The broader context for the US undertaking such strident measures against Russian activity in cyberspace — although critics claim that these steps are belated and will in fact have little effect — is that of the current global debate around legal and policy norms restricting state activity in cyberspace. Leaving aside the internal US politics of President-elect Trump’s actual implementation of the sanctions, there remain difficult dilemmas around the legal issues that arise when countries intervene with hostile intent in each other’s critical national infrastructures, whether these are physical or virtual, such as data and databases critical to the electoral process.

A number of international legal and policy processes have been initiated to address the crucial questions around states’ intervention in each other’s affairs, including what constitutes a prohibited use of force in cyberspace, what a “cyber attack” constitutes, giving rise to a nation’s right to self-defence under international law. For example, the 2013 Tallinn Manual, published under the auspices of NATO’s Cooperative Cyber Defence Center of Excellence (CCDCOE), sets out 95 rules on these and other issues, with commentary on the international law relating to their application. Other initiatives include the ongoing efforts of the UN Secretary-General’s Group of Governmental Experts, the Organization for Security and Cooperation in Europe (OSCE) and the Group of Seven (G7). China and Russia have also used a regional organization of their own, the Shanghai Cooperation Organization, to propose a draft treaty on global cybersecurity norms.

States and international organizations are still in the process of calibrating which types of activity are permitted and which are forbidden under international law in cyberspace. Traditional understandings of legal boundaries and their communication through diplomatic means are changing.

This latest Executive Order is an example of this task of calibrating the appropriate responses to hostile activity in cyberspace. It brings us to a watershed moment for cyber diplomacy and deepens our understanding of the normative boundaries of international behavior that nation-states will tolerate from one another in cyberspace.

—

Adv. Deborah Housen-Couriel is an Israeli attorney specializing in cybersecurity law and regulation. She works with a Tel Aviv cybersecurity consulting firm, Konfidas Digital and with Zeichner, Ellman and Krause LLC in New York and Israel. Deborah is also a research fellow at the Law Faculty of Haifa University, Tel Aviv University's Interdisciplinary Cyber Research Center and the Herzliya IDC's International Institute for Counter-terrorism. She can be reached at www.cyberregstrategies.com.

SPONSORED CONTENT

Recommended by

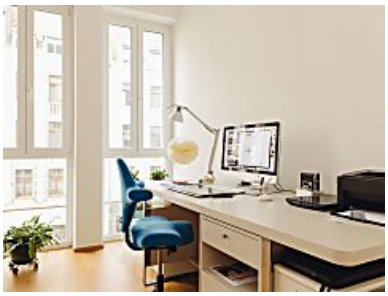
The Wedding planners at The Ritz-Carlton, Philadelphia
GQ

Luxury Bomber Jackets For High Spenders
Adam Express

The Ritz Carlton Philadelphia is an architectural landmark…
Vogue

Best Bomber Jackets On The Market
Adam Express

Eight Months with the Microsoft Surface Pro 4 –…
Gadget Guy Australia



How To Build a Professional Home Office
Mansion Global

SPONSORED STORIES

- 3 Blue-chip Shares I'm Avoiding in 2017
  (Motley Fool Australia)

FROM THE TIMES OF ISRAEL

- How to outmaneuver a tyrant
- The shape of things to come

- Medieval Pilgrim Excavated in UK Carried Leprosy Strain That Still… (GenomeWeb)
- DIY Hack: Calculate Customer Lifetime Value Using Excel (Optimove)
- Trump's Isolationism Offers Europe a 'Tremendous Opportunity' (Handelsblatt Global Edition)
- World's Most Expensive Home Hits Market for €1 Billion (Mansion Global)
- GoPro HERO5 goes flying into the cloud (Gadget Guy Australia)

- A chance meeting…..or was it?
- The Women Who Made Moses
- American Christians Take Up Our Cause
- Sigh of relief as Israel passes the tourist test

Recommended by

© 2015 THE TIMES OF ISRAEL, ALL RIGHTS RESERVED