The Heritage Foundation

ISSUE BRIEF

No. 4748 | AUGUST 3, 2017

Cooperation with China and Russia Is Not the Solution for Cyber Aggression

David Inserra

Cooperation with cyber adversaries is regularly floated as a way to lessen cyber attacks against the U.S. Under President Obama, the U.S. pursued a schizophrenic policy that promised cooperation and working groups with actors like Russia and China but also issued several high-profile condemnations of cyber attacks by those nations.

The Trump Administration has continued this confused approach. President Trump initially tweeted about working with the Russians to create "an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded." Thankfully, he subsequently redrew that idea. However, his advisers have continued to propose scaled-back forms of cooperation with Russia.

Cooperation with like-minded countries can and should be vigorously pursued, but U.S. leaders are fooling themselves if they believe that malicious cyber nations will agree to cease aggressive acts merely because of a new working group. Indeed, the potential costs of such cooperation outweigh any feasible returns. As such, policymakers should seek to significantly limit cyber cooperation with bad actors.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4748

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

A History of Ignoring Norms and Treaty Obligations

Trustworthiness is the first major problem when cooperating with nations like China or Russia on cybersecurity issues. China and Russia have proven through their actions in cyberspace and elsewhere that they will ignore norms, laws, and treaties when such behavior suits them. A brief search finds that Russia and China have serious difficulties honoring their commitments or basic norms.

Russia has:

- Rejected U.S. efforts to extradite or punish Russian hackers, even for routine criminal charges;
- Hacked U.S. political organizations and engaged in influence campaigns during the U.S. 2016 elections;
- Violated on multiple occasions the Intermediate-Range Nuclear Forces Treaty, culminating in the recent deployment of these prohibited nuclear weapons to threaten European allies;
- Violated the Presidential Nuclear Initiatives, the Chemical Weapons Convention, and likely the Biological Weapons Convention and the Comprehensive Test Ban Treaty;[1] and
- Violated various international agreements, including the Helsinki Final Act, the Budapest Memorandum on Security Assurances, and others, with the illegal annexation of Crimea and continued military involvement in Georgia, Moldova, and Ukraine.

China has:

- Violated the U.N. Convention on the Law of the Sea and the judgment of the arbitration panel regarding spurious Chinese territorial claims in the South China Sea;

- Ignored its obligations under the Sino-British Joint Declaration regarding the autonomy of Hong Kong, declaring that the agreement is a "historical document" that "no longer has any practical significance" and is "not at all binding" on China;[2] and

- Engaged in widespread, state-sponsored campaigns of cyber-economic espionage.

In fact, even when China and the U.S. came to an agreement on cyber-economic espionage, China steadfastly denied ever engaging in such cyber espionage. Furthermore, while economic espionage appears to have been reduced following the agreement, China has continued in violation of the agreement. Indeed, it was the threat of sanctions, not the promise of cooperation, that seems to have altered Chinese behavior. In other words, the exercise of U.S. power, not signing an agreement, appears to have resulted in changed behavior.

These lists only scratch the surface of Russian and Chinese transgressions, but they should sufficiently prove that U.S. efforts to engage with Russian and Chinese officials on cyber are misguided because no real agreement can be credibly established.

The Costs of Cooperation with Challengers

While Russian and Chinese history of ignoring international agreements should be a strong enough case to reject additional cooperation on cybersecurity on its face, there are also specific policy reasons why such cooperation is antithetical to U.S. interests.

Cybersecurity cooperation may reveal U.S. intelligence, processes, or mindsets that actually help its adversaries. Multiple experts and policymakers have condemned the proposal to establish some sort of cyber center with Russia, with some calling it the equivalent of letting the fox into the hen house under the pretense of guarding the hens.[3] The "fox," in this case, is just going to get fatter as it learns even more about U.S. cybersecurity efforts and how to undermine them.

Some have argued that such cooperation could be limited to the development of international cyber norms,[4] but the recent history of Russia and China clearly shows that international norms and agreements are little more than paper to these bad actors. The U.S. may take its international agreements seriously, but policymakers must not be fooled into believing that actors like Russia or China share its honesty or goodwill.

Cooperation with bad actors is not in U.S. interests because it continues a schizophrenic U.S. approach to international cybersecurity. During the Obama Administration, the U.S. alternated between punishing certain bad actors and accommodating them. Entering into cybersecurity cooperation with bad actors continues to show that the U.S. is not serious about handling such threats. Indecision and weakness in responding to malicious cyber actors will continue to invite more aggressive cyber actions.

Sending the Right Message

Rather than weaken U.S. cybersecurity, the U.S. should send a strong message that cooperation is only possible with credible, faithful partners. Seeing that China and Russia do not qualify as such, policy-

1. Franklin C. Miller and Keith B. Payne, "No More U.S.-Russian Arms Treaties Until Moscow Stops Violating Existing Treaties and Agreements," *RealClear Defense*, March 10, 2017, http://www.realcleardefense.com/articles/2017/03/10/no_more_us-russian_arms_treaties_until_moscow_stops_violating_existing_treaties_and_agreements_110946.html (accessed August 1, 2017).
2. Ben Blanchard and Michael Holden, "China Says Sino-British Joint Declaration on Hong Kong No Longer Has Meaning," Reuters, June 30, 2017, http://www.reuters.com/article/us-hongkong-anniversary-china-idUSKBN19L1J1 (accessed August 1, 2017).
3. Laura King, "Trump Doesn't Dispute Russia's Assertion He Was 'Satisfied' with Putin Response on Hacking," *The Los Angeles Times*, July 9, 2017, http://www.latimes.com/politics/washington/la-na-essential-washington-updates-trump-doesn-t-contest-russian-assertion-1499609801-htmlstory.html (accessed August 2, 2017).
4. Andrew Blake, "U.S. and Russia Must Discuss 'Rules of the Road' Before Pursuing Cyber Pact: Trump Security Advisor," *The Washington Times*, July 14, 2017, http://www.washingtontimes.com/news/2017/jul/14/us-and-russia-must-discuss-rules-of-the-road-befor/ (accessed August 2, 2017).

makers must limit cooperative ventures and instead rely on various tools of national power to appropriately punish cyber aggression. Therefore, Congress should:

- **Restrict military cyber cooperation with Russia and China.** The Senate is set to take up the National Defense Authorization Act (NDAA) in the coming weeks. The Senate should restrict the Department of Defense from spending any money on any activity where the primary purpose is to engage in cyber cooperation with Russia and China. An exception can be made for so-called hotlines or other emergency communications but broader cooperative efforts should be forbidden.

- **Use all tools of national power to retaliate against acts of cyber aggression.** Rather than continuing to seek cooperation, the U.S. should pursue a consistent strategy of punishing cyber aggression. Given that China and Russia are untrustworthy, only the exercise of U.S. power can curtail their malicious cyber activity. Naming and shaming, legal action, financial restrictions, sanctions, seeking trade remedies, and other strategic responses should be used as appropriate to punish bad actors.[5]

- **Increase cooperation with allies and partners.** Many cyber attacks and incidents will not be punishable, but instead require stronger defenses and cooperation to defeat or mitigate. Russia and China are not credible partners, but the U.S. can and should pursue deeper technical, legal, and policy cooperation with its allies and partners.

Advancing U.S. Cybersecurity

The U.S. has been the victim of cyber aggression for far too long with far too small a response. When dealing with malicious cyber states, the solution is not to strengthen and embolden them but to punish them. Together with increased cooperation with allies and partners, U.S. policymakers can make cyberspace more secure.

*—**David Inserra** is a Policy Analyst for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

5. David Inserra, "Cybersecurity Beyond U.S. Borders: Engaging Allies and Deterring Aggressors in Cyberspace," Heritage Foundation *Backgrounder* No. 3223, July 14, 2017, http://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors.