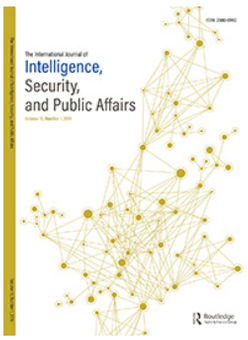

The International Journal of Intelligence, Security, and Public Affairs

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/usip20

A Study in Complexity: Unintended Consequences of Multiple Stakeholders in the U.S. Presidential Election Process

Richard J. Chasdi & Sheila R. Ronis

To cite this article: Richard J. Chasdi & Sheila R. Ronis (2020): A Study in Complexity: Unintended Consequences of Multiple Stakeholders in the U.S. Presidential Election Process, The International Journal of Intelligence, Security, and Public Affairs, DOI: 10.1080/23800992.2020.1840801

To link to this article: https://doi.org/10.1080/23800992.2020.1840801

Published online: 05 Nov 2020.

THE INTERNATIONAL JOURNAL OF INTELLIGENCE, SECURITY, AND PUBLIC AFFAIRS
https://doi.org/10.1080/23800992.2020.1840801

A Study in Complexity: Unintended Consequences of Multiple Stakeholders in the U.S. Presidential Election Process

Richard J. Chasdi[a] and Sheila R. Ronis[b]

[a]Department of Political Science, George Washington University, Washington, DC, USA; [b]Ohio State University, Columbus, OH, USA

ABSTRACT

In 2023, 3 years after the 2020 U.S. Presidential election, a select group of senior intelligence analysts from the National Security Agency (NSA), Department of Homeland Security (DHS), and the Office of National Intelligence met for a reunion at an undisclosed location in Virginia to recall their all-day meeting with the National Security Council (NSC) at the White House in May 2020, and to recount the watershed international events that lead to the election of President Joseph R. Biden, Jr.

ARTICLE HISTORY
Received 4 August 2020
Revised 2 October 2020
Accepted 17 October 2020

KEYWORDS
Cyber Warfare; National Security Agency; intelligence

In 2023, 3 years after the 2020 U.S. Presidential election, a select group of senior intelligence analysts from the National Security Agency (NSA), Department of Homeland Security (DHS), and the Office of National Intelligence met for a reunion at an undisclosed location in Virginia to recall their all-day meeting with the National Security Council (NSC) at the White House in May 2020, and to recount the watershed international events that lead to President Joseph R. Biden Jr.'s election.

Josephine Clarke, an NSA intelligence analyst, and her counterparts Jonathan Edwards from CIA, Charles Goodwin of DHS, and Timothy Burke from the Office of the Director of National Intelligence (ODNI), recalled that evening in late June when an encrypted memo marked Top Secret was sent. In it was a description of the spike in the frequency, and in some cases, intensity, of the cyber-terrorist assaults carried out over the past 4 months against the United States. This cable would serve as the topic of analysis, and an invitation to the White House scheduled right before Independence Day, July 4, 2020.

The communique received revealed the mission: to rank probabilities as to the goals (i.e., purpose), sources, and root origins of those cyber-assaults, by means of a cyber-attack event content analysis that used quantitative and qualitative algorithms to find contextual similarities between those cyber-attacks, and the watershed American events that happened. Those events included shifts and

CONTACT Richard J. Chasdi rchasdi@aol.com George Washington University, Washington, DC

formations of coronavirus epicenters, and high-profile acts of police abuse. Lag times between those events and cyberattacks were to be determined, as was the mix of national and state political institutions hacked into, and the geographical locations involved.

The analysis requested by NSC officials and staff was not limited to public sector targets. The cyber-assaults detected also included attacks against MNCs, other international enterprises, and domestic small and middle size enterprises (SME's), as well as non-governmental organizations. The frequency, intensity, target characteristics, and similarities in cyber-protection vulnerabilities had to be plotted. In addition to ransomware attacks, the analyst team learned more about some of the specifics upon arrival: the cyber-assaults under consideration also included "buffer overflow attacks," where computer systems crashed because memory capacity was overwhelmed with high volumes of Internet activity (Chasdi, 2018, pp. 124–177).

Clarke, Edwards, Goodwin, and Burke all had deep understandings of the national security risks involved. Each analyst understood that in a world characterized by coronavirus and increasingly sophisticated cyber-assault capabilities, some authoritarian regimes recognized opportunities to take cyber-intrusion actions against the United States in the fierce ideological struggle with many Western countries about the merits and advantages of Western-style liberal democracy. At a functional level, the reason why those attacks were orchestrated was to sow profound and lasting discord in American society. American adversaries understood that cyber-attacks worked well to amplify the political and economic inequality effects in the American political system, where enshrined individual liberties and civil rights are guaranteed, at least theoretically, but where economic rights, especially critical for disenfranchised Americans, remain largely ignored.[1]

Clarke, in one of the first tabletop exercises conducted, surmised that cyber-attacks against key American industries such as Boeing, Raytheon, and Tesla were designed to impede any prospect of progress toward some semblance of economic recovery after the COVID-19 pandemic hit in January 2020. Plainly, the coronavirus pandemic, compounded by the Trump administration's ineptitude, had devastated the U.S. economy; those cyber-assaults only worked to increase job loss, unemployment claims, and push the U.S. economy into a condition of negative growth.

Clarke, herself a formally trained economist, presented persuasive evidence those cyber-attacks were carefully reasoned and carefully planned; designed to increase economic hardship and political tensions in the midst of a biological calamitous condition. She cited a *Congressional Research Service* report (September 2020), where in May, Federal Reserve Chairman Jerome Powell stated that over 20 million workers in the U.S. were unemployed due to the virus. The report also mentioned that 61 million U.S. workers applied to receive "unemployment insurance" benefits between the middle of March and the

middle of September 2020, while the official U.S. unemployment rate in April 2020 was 14.7%. (Congressional Research Service, 2020, pp. 1–3, 14; Federal Reserve Board, 2020, p. 1). All that intensified the type of political instability that undercut Western-style liberal democracy. As Edwards commented to his colleagues, such economic hardship meant increased tensions and instability between the "haves" and "have-nots" that in turn, would lead to higher probabilities of protest, associated violence, and police violence as a response.

One conclusion drawn at that NSC meeting was that the nation-state leadership behind those attacks was familiar with "complex systems theory," with its underlying theme that an operational system, in this case, the United States and under cyber-attack assault, would be extremely vulnerable because of connections and interdependencies between government, non-state actor stakeholders, such as the "Black Lives Matter" movement, and explanatory factors, such as constituent support, outside finances, and "exogenous shocks" to the system, such as cyber-assaults. In a "complex system," a change in stakeholder(s) process or explanatory variables can produce "first order" system effects that can elicit "second order," "third order," and "fourth order" ripple effects (Fuerth & Faber, 2007; Ronis, 2007).

Analysts understood what was widely known, namely that violent "right-wing" groups had used the coronavirus as a springboard to launch anti-Semitic and racist attacks directed at Asian-Americans and African-Americans, oftentimes in convoluted narratives that described efforts at world domination led by the American political left. However, what was not widely documented at the time was that political instability in American society, itself a "second order" coronavirus effect that exacerbated American political and economic inequalities, had already been appraised as a powerful explanatory factor in the complex system analyses run by Case, Burke, and other analysts (Diamond, 1990, 351-409).

What intelligence agency analysis had illuminated was that "second order" effects from police killings within the context of coronavirus increased tensions between moderate and radical "Black Lives Matter" leaders, that in turn led to a "third order" effect: the increasing likelihood that "Black Lives Matter" radicals would splinter to form new more radicalized groups. What concerned analysts was the role of another important non-state actor, and its contribution to that process, namely the Nation of Islam led by Minister Louis Farrakhan. The ineluctable conclusion was that the prospect of Farrakhan's involvement with monetary incentives and covert training to "Black Lives Matter" radicals made "fourth order" effects much more likely: an unprecedented formation of new U.S. terrorist groups determined to attack the U.S. government.

In fact, Goodwin and Burke knew the FBI, working in conjunction with Illinois, Kentucky, and Michigan state police intelligence units, had conducted

operations that determined a series of clandestine meetings known only to Farrakhan and to "Black Lives Matter" militants, had already taken place in early July, without the endorsement or knowledge of "Black Lives Matter" officials. Goodwin (DHS) and Burke (ODNI) had been one of the first to tell Edwards (CIA) and Clarke that the first phase of a new classified set of counterterrorism policies had been implemented, designed to enhance "Black Lives Matter" cohesion and nearly simultaneously, to inhibit "Black Lives Movement" splinter effects (Chasdi, 2020, pp. 119–131, 2002, pp. 77–78, 408–411, 417–418, 1999, pp. 84, 207–209, 216–219).

Clarke, who had grown up in the Mid-West, grimaced as she heard this, thinking about the time when she was eleven and the Students for Democratic Society (SDS) splintered to form the Weatherman (Underground), that appeared in 1969 at the University of Michigan. Clarke's fear was essentially the same; that "Black Lives Matter" would splinter to form one or more terrorist groups when the "defund the police" movement failed, or when the substance of the police reform bill before Congress was eviscerated by U.S. Senate Republican leadership.

The meeting at the White House had started out with an events chronology and description of the major events that happened since March 2020. Broader trends in attack patterns were not hard to discern – as the November 2020 U.S. presidential election approached, it was during the summer of 2020 that leadership in Moscow, Tehran, Pyongyang, and Beijing realized independently that two recent events, considered acts of U.S. state terrorism against people of color by some analysts, had produced a propitious time to accelerate cyber-intrusions to disrupt U.S. elections.

Those proximate watershed events included the videotaped May 20, 2020 murder of George Floyd by Minneapolis police, the shooting death of Breeona Taylor by police in Louisville, Kentucky on March 13, 2020, and the widely broadcast videotaped death of Elijah McClain in Aurora, Colorado by police on August 19, 2019. Another pivotal event that contributed to strains and tensions, was the murder of Ahmaud Arbery in Brunswick, Georgia, committed by an ex-policeman and his son. From the start, the disruption of U.S. elections to give Trump an advantage over his Democratic rival had been the aim of Russian, Iranian, North Korean, and Chinese leaders; it traced an arc back to the election of President Donald J. Trump in 2016.

There was a general consensus at the NSC meeting that for President Vladimir Putin, this virtual cyber-intrusion campaign to undercut Democratic nominee Vice President Joe Biden reflected past patterns of warfare behavior. This new cyber-attack campaign was of particular significance because of Russian national interests, particularly in the Middle East, in Syria and Libya. Plainly, the use of cyber-attacks and other methods such as the disinformation campaign about Hunter Biden's business dealings had become a Putin strategic initiative after 2016 to undercut political support for Biden, and for particular Democratic congressional and gubernatorial candidates.

Indeed, Russian cyber-assault expertise had been refined and its mettle has been proven over years with experience. The cyber-assault campaigns during the 2016 U.S. Presidential election, with Federal Security Service (FSB) and Main Intelligence Directorate (GRU) cyber-intrusions against the Democratic National Committee (DNC) and its affiliate, the Democratic Congressional Campaign Committee, had built on lessons learned from previous events. Those included Putin's cyber-assaults in Estonia (2007); Russian cyber-assaults used by President Dimitry Medvedev and Prime Minister Putin in the Russo-Georgian War (2008), and most recently, Putin's use of cyber-assaults in 2019 against Georgia (White, 2018; Chasdi, 2018, pp. 29–33, 194 n34, 35–36).

The NSC meeting analysts worked to decipher Putin's motivations behind those cyber-assaults. Many analysts believed Putin's appraisal, that concluded Biden's election would result in new, tougher U.S. foreign policy initiatives against Russian, Syrian, and Iranian geopolitical interests, would also make use of positive inducements offered to Turkey's President Rycep Tayyip Erdogan. Analysis suggested Putin thought positive inducements to Turkey might include tacit approval for Erdogan to confront Syrian President Bashar al-Assad, and Iran's Ayatollah Khamenei over Euphrates and Tigris river water rights.

It was also surmised that Putin believed a Biden victory promised much stronger support for the U.N. recognized Government of National Accord (GNA) in Libya, led by Prime Minister Fayez al-Sarraj. This was also the government that was strongly supported by Erdogan; that gave the Americans additional leverage for action. Thus, ran the argument, Biden could strengthen ties to Erdogan in support of Sarraj, and in opposition to the Tobruk government.

For Putin, this was for Biden, a logical move given existing U.N. support for the Tripoli government in its struggle against General Khalifa Haftar and the Libyan National Army (LNA), and because of several Government of National Accord (GNA) victories over Haftar's LNA in the spring of 2020. Clarke, Edwards, Goodwin, and Burke, as well as the NSC members were in agreement about the purpose behind Putin's assaults. Their analysis suggested that from Putin's crow's nest, Erdogan was the pivotal actor – if Biden was elected, the leverage he had over Erdogan amounted to a series of coercive diplomacy "limited options" that included the threat to reestablish relations with the Syrian Democratic Forces (SDF), severed by Trump (Powell, 1990, pp. 1–33).

The analysis suggested Putin experienced consternation over that prospect – Biden could also ratchet up the pressure, should the foregoing threat be insufficient to coerce Erdogan to comply, by holding out the possibility of U.S. support for an autonomous area in northern Syria, led by the Kurdish dominated People's Protection Unit (YPG) (Powell, 1990, pp. 1–33). What was significant was that in October 2020, Putin's intelligence operatives at the GRU had discovered a draft of an internal Biden campaign memo that advocated

that a newly elected President Biden might also offer Erdogan an initial confidence building measure (CBO) – an offer to put new pressure on the Saudis to take responsibility for Jamal Khashoggi's murder in Turkey, in exchange for greater Turkish cooperation. Plainly, all this concerned Putin and ramped up the pressure for him to ensure a Trump victory in November (Baldwin, 1971, 1985). Thus, Putin's cyberattacks had primarily short-run goals in mind.

As the meeting in the White House progressed, it became clear China's President Xi had also authorized a series of cyberattacks directed against American assets. However, unlike the Russian case, the purpose and reasoning behind those attacks were more nuanced, precisely because of the set of intricate and continuously evolving economic connections between the United States and China. Goodwin, the economist in the team, explained the interconnectivity between those countries; China had become the world's leading energy importer and the United States a leading exporter of energy due to its non-traditional shale oil production and new influence over many oil producers.

Hence, President Xi had to straddle the geopolitical line between more proximate demands of working to ensure President Trump's reelection and long-haul Chinese geo-strategic economic interests that remained heavily interdependent with the United States. Burke and many of his colleagues stressed that point repeatedly, arguing that "issue areas in international politics are interrelated"; with conflicts between the United States, Japan, and China that worked to provide policy intervention opportunities for the Americans to exploit with the use of both "carrots" and "sticks," to attain compliance. Those issues included, but were not limited to, littoral and territorial control in the South China Sea, tensions between the Indian government and President Xi over disputed borders in the Himalayas, and the futures of Hong Kong and Taiwan.

Still, as Edwards, an expert of Chinese politics argued forcefully, President Xi probably believed he held control over the penultimate threat that would ultimately restrict American actions against him – the threat to sell vast amounts of U.S. financial debt held by China, especially to nation-states with interests antithetical to those of the United States. The central notion was if that threat was ever enacted or even issued, it would precipitate enormous plunges in stock markets that could lead to financial market collapse world-wide, and ruin American NASDAQ and Dow Jones stock market exchange performance.

As Clarke and several of the political scientists on the NSC staff noted, while that fall back plan to sell U.S. debt seemed a formidable deterrent for President Xi against the prospect of U.S. action in response to Chinese cyberattacks, it did not take into account how that plan would only amount to a Chinese Pyrrhic victory, precisely because of the economic interdependencies between

both countries. It also did not take into account the potential of American preemptive action in cyberspace, or the use of military actions, including those in space carried out by Trump's New "Space Force," should political and diplomatic options to confront the Chinese prove ineffective.

Hence, Burke, a formally trained political scientist, stressed the importance of what David Baldwin calls "positive sanctions." Burke explained that Baldwin's "positive sanctions" amounted to a mix of positive inducements and "negative sanctions" used by a state or non-state actor, either simultaneously or sequentially, to produce "a baseline of expectations" (Baldwin, 1971, 1985; Powell, 1990, pp. 1–33). Burke drew heavily on Baldwin's work to argue that the U.S.-Chinese relationship was "too big to fail" and that use of a mix of "positive sanctions" with traditional negative sanctions introduced greater flexibility into that political relationship, by working to create a greater range of U.S. policy alternatives.

It was at this point in the meeting that analysts crafted a "cyber-attack motivations continuum" to depict the different motivations, range of targets, and characteristics of the cyber-assault threats. NSC officials believed that a depiction and categorization of those threats would serve as a basis for policy options. The continuum was defined by two dimensions – the first was "Goal Clarity" – to capture the singularity or straightforwardness of U.S. adversary objectives. An ordinal scale (1–10) captured the range, from complete "opaqueness" (1) to pure "clarity" (10). It was found that an increase in the quality of goal opaqueness was a function of the interdependency of specific issues across broader political and economic issue areas. The second dimension of this continuum was "Time Frame" – a scale to capture whether the political objective under consideration was "short-run," "middle-run," or "long-haul."

In the case of "Goal Clarity," Russia scored high, while in the case of time frame, the political objective was "short-run" – to ensure Trump's reelection. As the meeting progressed, it became clear the Chinese case (with its interconnected political and economic context) represented a different case, that if depicted on this continuum, would fall almost at the opposite end of the spectrum from where the Russian case was placed. Chinese goals were opaque rather than clear, and only partially understood, but that condition plainly reflected the myriad of economic and political interdependencies that characterized the broader relationship between the United States and China. If the Russian case had short-term goals, then the Chinese case, by contrast, had long-haul objectives.

The NSC meeting continued after a break for lunch. When attendees reconvened, additional work on goals and motivations within the context of this continuum made it clear that the cyberattacks that emanated from Iran and North Korea could be placed at points on the continuum between its two axes, Clear Goals – Short-Run Time Frame, and Opaque Goals – Long-Haul Time Frame. Clarke and others in charge of analysis of Iranian cyber-attacks

noted that Iran's use of cyber-attacks had a narrower range of motivational factors and implied goals, primarily oriented toward its conflict with Israel and Saudi Arabia. However, there was a range of stakeholders involved. That included Turkey with its"Neo-Ottomanism" policy, that was broader than those in the Russian case.

Clarke's tabletop exercise team noted that Iranian cyber-assaults scored high on the dimension of "clarity" – those were relatively straightforward, motivated by hatred and anxiety about Trump's hyper-aggressive Iranian policy, Israel, and Saudi Arabia. Examples of that hyper-aggressive policy included the murder of General Qassem Suleimani and Popular Mobilization (PMF) militia chieftain Abu Mahdi al-Muhandis, Trump's "maximum pressure" sanction policies, Trump's strong pro-Israel policies, his insouciance about Crown Prince Mohammed Bin Salman al Saud, and the Saudi acquisition of ballistic military technology, presumably from the Chinese government.

To be more specific, the analysts at that meeting believed the central notion behind those Iranian cyber-assaults was fourfold: to demonstrate Iranian cyber-security capacities and their improvement since the Stuxnet affair (2010); to underscore how the U.S. is unable to protect its citizens from the domestic political instability that followed those cyber-assaults; to demonstrate the potential damage possible from Iranian cyber-assaults if aimed at U.S. infrastructure, such as energy and communication facilities. The fourth dimension of those Iranian attacks with its strong cyber-capabilities, was to improve the Iranian political position because the Iranians, as were the Americans, continued to jockey for position in the bargaining process about new diplomatic agreements in the aftermath of the Joint Comprehensive Plan of Action (JCPOA) debacle (Wagner, 2007, pp. 105–129; Fearon, 1995, pp. 379–414; Snyder, 1984, pp. 461–494). Thus, with respect to goals, analysts determined that Iran had a middle-run time interval timeline.

In the case of Pyongyang, the results presented by Case, Edwards, Goodwin, Burke, and their NSC colleagues reflected a greater difference in opinion about the goals, time line, and determinants behind the spate of North Korean cyber-attacks. Some analysts in the North Korean table-top exercise team argued that this case involved a greater mix of domestic and international political factors than the other cases. There were lingering questions about the health of Kim Jung Un and the instability that followed, especially with the rise of Kim's sister to higher levels of power; that was believed to be a contributing factor to this set of North Korean cyberattacks. The analysts concluded the central idea was to promote the ideals of strength, that in operation, were necessary to repel any sort of American supported military action against the regime. It appeared that while the level of "goal clarity" was low, with a mix of domestic and international issues in play, a long-haul time frame was involved, that revolved around the Kim regime's survivability.

All four analysts reflected on the theoretical and investigative complexities associated with their mission, but soon discussion turned to the extremely dangerous and de-stabilizing set of cyber-assaults themselves that happened shortly after July 4, 2020. Clarke was particularly overcome with emotion as she recalled events: what followed shortly after that NSC meeting were a series of "false flag" cyber-intrusion events where state government hackers impersonated different stakeholders in the American political system to antagonize others. These attacks were directed against the government, business, and nongovernmental organizations to stoke racial, ethnic, and religious tensions in the United States.

One prominent "false flag" cyber-attack was aimed at Reverend Al Sharpton who was impersonated online with corresponding spliced film footage from past events to make it appear Sharpton was berating Jews for their general indifference and lackluster support for the "Black Lives Matter" movement. As if that were not enough of a problem, that disinformation compounded strains and tensions already produced in the spring of 2020 by "right-wing" activists who argued the coronavirus was the product of the liberal "left-wing," working in conjunction with Jews to promote Jewish and progressive world domination (Anti-Defamation League, 2020, n.d.).

In turn, impersonators of Jewish academics conveyed similar sentiments on social media, with emphasis on the underlying theme that "all lives matter." Nearly simultaneously, the Anti-Defamation League (ADL) and B'nai Brith also experienced similar "social engineering" or impersonation endeavors. Another cyber-attack targeted Vice President Joe Biden with a fictitious portrayal of an African American woman accusing Biden of rape, around the same time that Tara Reade had alleged that Biden molested her in a Congress office building hallway.

These efforts were not only limited to attacks designed to exacerbate tensions between race, ethnicity, political ideology, and men and women – there were also "false flag" attacks designed to enhance the effects of American socio-economic divisions. One prominent campaign spliced footage of Mitt Romney, during his now infamous statement about "the one percent of Americans" who were his concern, surrounded by local and state Democratic officials in a new meeting with its purported aim of making subservient the American working class for generations to come. The underlying theme to all this was to divide the democratic electoral base, and in the process, elicit the type of fundamental protests against the white liberal establishment, that would mirror protests against white conservative leadership in the U.S. Congress and at gubernatorial levels, who continued to uphold Trump's tacit support of police brutalities against people of color.

Even though some of those early cyberattacks in this slew of uncoordinated events were effective, helping to produce the political instability and social unrest seen over the summer of 2020, these attacks were readily traceable to points of

origin. Every analyst at the NSC meeting understood that each cyber-assault left a distinct set of malware signature trails for American cyber-attack experts at NSA and DHS to exploit. Efforts by EUROPOL and domestic law enforcement agencies in certain "friendly" Eastern European countries revealed computer hackers had worked in conjunction with leaders in Tehran, Pyongyang, and Beijing to craft those cyber-attacks and obscure sources or origin.

The use of non-state actor hacker communities, employed to help obfuscate the origins of those cyber-assaults proved to be the Achilles heel of these cyber-terrorism campaigns. One Russian hacker organization involved, known as the "Minsk Malicious Malware Group" (MMMG), originally worked both sides to playoff democratic and non-democratic regimes. It was that hacker group's participation and eventual disagreements with Russian authorities over inadequate monetary compensation, that led to the MMMG's closer involvement with the United States Department of Homeland Security (DHS), and subsequent revelations about Russian plans; that broke open the entire set of sustained but uncoordinated operations.

All of the foregoing constituted a crisis that required a carefully reasoned set of American response actions taken within a limited time horizon. Tailor-made responses were crafted for each country for several important reasons. The governments behind those cyber-attacks in Russia, China, Iran, and North Korea were characterized by different political, military, and economic vulnerabilities that derived from the "contextual factors" of each country. For example, Iran was characterized by multiple borders, hostile neighbors, and minority groups that analysts believed could be mobilized with American support to destabilize Iran's government if necessary (Jervis, 1978, pp. 172–173; Waltz, 1973, pp. 10–20).

North Korea was also surrounded by hostile neighbors, but it differed from the Iranian case because North Korea had few natural resources, and an even more restless population, deprived of the basic necessities of life. American analysts also believed that like some of the minority groups in Iran and some of Iran's population, some North Koreans were ripe for political incitement. As North Korea's leadership goals from their cyber-attacks were deemed long-haul objectives, threats of support for North Korean insurgencies were potentially a powerful tool in the context of perceived instability due to Kim's health.

In the case of Russia, even though Russia had enormous size and plentiful resources that contributed to its security, it was surrounded by several borders and had restless populations to contend with in the Caucuses, especially in the Russian republics of Chechnya, Ingushetia, and Dagestan (Jervis, 1978, pp. 172–173; Waltz, 1973, pp. 10–20). Threats to support Islamic self-determination in that region provided that local leadership in those areas sever allegiances with ISIS, was seen as a potent American policy threat against Putin.

It was China that posed some of the most difficult challenges in terms of response, precisely because of its interdependencies with the United States, and the knowledge that with China's emergence as a superpower, the U.S. would have to contend with China and find some form of "peaceful co-existence" for a long time to come. Because of those complexities, Clarke talked about the importance of short-run measures even within the context of long-haul Chinese motivations and goals. She spearheaded a short-run campaign to tackle the Chinese problem through Iran, thereby in effect working to confront the cyber-assault challenges that each country posed.

Clarke's plan was to confront Iran and China in cyberspace, by having the National Security Agency (NSA) in conjunction with the CIA work to manipulate the computer code signatures of attacks that emanated from each country, to make it appear that Iranian leaders, interested in the expansion of their influence, supported the Uighur community's political demands and aspirations for increased autonomy, if not independence outright. Many American intelligence officials thought this two-pronged approach to link threats posed by Iran and China to craft a disinformation campaign might be successful because of previous intelligence reports received about Iranian national interest objectives. Those reports suggested Iranian leaders believed they could make successful overtures to India because closer ties to India would help increase Iranian influence in Afghanistan, where both the Indian and Pakistani governments continued to jockey for a political position.

The Iranians believed that they could serve as an interlocutor for both India and China, whose military forces recently had a series of border dispute skirmishes in the Himalayas; the idea was that in the process, Iran's leaders could curry favor with leaders both in Delhi and in Beijing. For Ayatollah Khamenei and President Rouhani, there was another "push factor" involved – Pakistan. Events in Pakistan since the death of Osama bin Laden in Abbottabad led to the ineluctable conclusion by Iranian leaders that Pakistan, with its own internal problems such as crime, terrorism, poor governance, and substantial support for Sunni Islamic extremism, had become too unpredictable and unstable for Iran to maintain a full-blown alliance with Pakistan.

All of this galvanized into a plan for the Americans to create a set of "false flag" cyber-assaults of their own. What was significant was that American domestic factors, not readily discernable to the American public, contributed to the implementation of this policy. U.S. Secretary of Defense Mark T. Esper, long perceived as a Trump sycophant by the U.S. public, and increasingly disillusioned with Trump's overall leadership, decided to promote the plan with the tacit support of many U.S. intelligence agencies. Trump, himself overwhelmed with his inability to cope with the COVID-19 crisis, and domestic political fallout from the "Black Lives Matter" movement, issued a pro-forma endorsement of the plan, without reading the plan carefully.

The basis of the plan was this: the computer codes of the Iranians, that had been broken months before, were utilized by NSA and DHS to manufacture disinformation about covert Iranian supported militias that had infiltrated into Xinjiang Province. The rationale provided was that Iran could not stand by and watch Muslims interred into what some called "concentration camps." Next, the Americans manufactured bogus Chinese diplomatic cables threatening retaliation against Iran, followed 4 days later by an American "false flag" cyber-attack of "Chinese origins" carried out against Tehran.

That U.S. "false flag" cyber-attack, which destroyed several electrical grids in the Tehran area, immobilized the Iranian leadership and panicked Iran's citizens. Its goal was to provide a signal to the Iranian ruling elite about the prospect of further "Chinese" cyber-attacks as a harbinger of events to come, should Tehran persist in its support of the Uighers. The Iranians were furious – in turn, Ayatollah Khamenei and President Rouhani cut off 50% of its clandestine oil shipments to China that had been shipped through third parties to avoid U.S. led sanctions, and the Iranians threatened further actions (Hsu & Morello, 2020, pp. A-18).

At the same time, after notifying India's Prime Minister Narendra Modi of the plan, an Esper directive authorized manufactured intelligence be sent to the Chinese to indicate that the Indian government had issued a general mobilization of its military after incidents of armed conflict between Chinese and Indian forces continued in the Himalayas. The Chinese, now feeling economic pressure from Iran with the Iranian government's decision to cut its Chinese oil supply, and military pressure from India, began their own militarization, even as international pressures led by U.N. Secretary-General Antonio Guterres to stand down grew apace within the context of the international COVID pandemic.

Finally, to complete the plan, the North Koreans were sent false information to suggest the United States government viewed Kim Jung Un's health problems, his sister's rise to power, and overall uncertainty about the regime's future, as a propitious moment for the United States to attack and destroy North Korean nuclear facilities. The threat issued was that in conjunction with those American military attacks, the United States would sign off on a limited South Korean military attack, to serve as a distraction for the American bombing of those facilities to come. Thus, the onus was placed on the Chinese, already on the horns of a security dilemma with Iran, and increasingly with India over territorial issues, to restrain the North Koreans and prevent a full-blown war with South Korea.

In the case of Russia, the Americans decided to act after accusations in June 2020 that Putin offered bounties on the heads of American soldiers and their allies proved to be true (Higgins & Kramer, 2020). Trump, concerned his reelection bid was on the cusp of complete failure, linked this issue to Russian cyber-attacks; he did a volt- face on G-7 expansion to exclude Russia; Trump

also authorized American intelligence agencies to manipulate the code of Russian cyber-attacks to create a disinformation campaign. That disinformation campaign made it appear to Putin that the Chechens, in conjunction with Muslim insurgents in Dagestan and Ingushetia, were on the cusp of a full-blown rebellion against the Russian government.

What was also compelling for Trump was this disinformation campaign, that led to Russian mobilization of its military forces, detracted from Putin's abilities to influence events in Libya, where the Russians had continued their overt support for General Khalifa Haftar and the Tobruk government. In a seemingly unrelated event, the United States Department of State announced that secret talks between the United States and Finland resulted in a Memo of Understanding between American and Finnish leaders about formal admittance of Finland into NATO.

To be sure, this was a very dangerous policy. The relationships between China and Iran, China and India in the Himalayas, China and North Korea, and Russia and the United States had become increasingly unpredictable and uncontrollable. As much as U.S. Defense Secretary Esper understood the risks involved, he was willing to take them because he, like many U.S. intelligence agencies, believed that the future of American democracy largely depended on getting tough with Putin. Trump, who had his own reasons to support the plan, had remained largely silent as all of the foregoing unfolded.

Still, the emergent reality was clear to Trump, who loathed to get tough with Putin, but knew that his prospects for reelection after the Russian bounty scandal were dim unless he initiated a structural shift in his relationship with Putin. His reelection fears outweighed the fears of Putin's retaliation – after all, he had only one term left. Hence, Trump quickly scheduled a U.S. television appearance to announce those dangerous international political conditions had been manufactured by the United States, both as a signal to indicate to potential adversaries what U.S. cyber-forces could orchestrate should the Americans choose to precipitate conflict in specific parts of the world, and as a singular shot across the bow to the countries behind those cyber-assaults. In the end, the U.S. national election went off without a hitch.

Note

1. That condition breathes life into the basic conundrum that critics note in John Locke's, *The Second Treatise of Government* (1690), a work of political theory at the bedrock of the American political edifice – namely the inability to achieve political equality without economic equality, or at least basic ranges of guaranteed economic security.

References

Anti-Defamation League. (2020, March 26). White supremacists respond to coronavirus with violent plots and online hate. *Anti-Defamation League*. Retrieved from https://www.adl.org/blog/white-supremacists-respond-to-coronavirus-with-violent-plots-and-online-hate

Anti-Defamation League. (n.d.). ADL report exposes right wing terrorism threat in the U.S. *Anti-Defamation League*. Retrieved from https://www.adl.org/news/press-releases/adl-report-exposes-right-wing-terrorism-threat-in-the-us

Baldwin, D. A. (1971). The power of positive sanctions. *World Politics*, *24*(1), 19–38. doi:10.2307/2009705

Baldwin, D. A. (1985). *Economic statecraft*. Princeton, New Jersey: Princeton University Press.

Chasdi, R. J. (1999). *Serenade of suffering: A portrait of Middle East terrorism, 1968–1993*. Lanham, MD: Lexington Books.

Chasdi, R. J. (2002). *Tapestry of terror: A portrait of Middle East terrorism, 1994–1999* (pp. 77–78, 408–411, 417–418). Lanham, MD: Lexington Books.

Chasdi, R. J. (2018). *Corporate security crossroads: Responding to terrorism, cyberthreats, and other hazards in the global business environment*. Santa Barbara, CA: ABC-CLIO; Praeger Press.

Chasdi, R. J. (2020, June). Research note- the new frontier on enhanced terrorism with the United States in mind. *The International Journal of Intelligence, Security and Public Affairs*, *22*(2), 119–131. doi:10.1080/23800992.2020.1780075

Congressional Research Service. (2020). Global economic effects of COVID-19 - Updated September 21, 2020 – R46270. *Congressional Research Service*, Washington, DC: United States Government. Retrieved from https://crsreports.congress.gov/product/pdf/R/R46270

Diamond, L. (1990). Nigeria: Pluralism, statism, and the struggle for democracy. In L. Diamond, J. L. Linz, & S. M. Lipsit (Eds.), *Politics in developing countries: Comparing experiences with democracy*. Coulder, Colorado: Lynne Rienner.

Fearon, J. G. (1995). Rationalist explanations for war. *International Organization*, *41*(3) (Summer), 379–414. doi:10.1017/S0020818300033324.

Federal Reserve Board. (2020, June 16). Semiannual monetary policy report to the congress – Chair Jerome H. Powell. *U.S. Federal Reserve*. Retrieved from https://www.federalreserve.gov/newsevents/testimony/powell20200616a.htm

Fuerth, L., & Faber, Evan M. H. (2007). *Anticipatory governance practical upgrades: Equipping the executive branch to cope with increasing speed and complexity of major challenges*. Washington, DC: National Defense University, Center for Technology & National Security Policy.

Higgins, A., & Kramer, A. E. (2020, July 4). "Russia denies paying bounties, but some say the U.S. had it coming." *The New York Times*. Retrieved from https://advance-lexis-com.proxygw.wrlc.org/api/document?collection=news&id=urn:contentItem:608J-M051-JBG3-6325-00000-00&context=1516831

Hsu, S. S., & Morello, C. (2020, July 3). U.S. acts to seize Iranian oil meant for Venezuela. *The Washington Post*,pp. A–18.

Jervis, R. (1978, January). Under the security Dilemma. *World Politics*, *30*(2), 167–214. doi:10.2307/2009958

Powell, R. (1990). *Nuclear deterrence theory: The search for credibility* (pp. 1–33). New York: Cambridge University Press.

Ronis, S. R. (2007). *timelines into the future: Strategic visioning methods for government, business and other organizations*. Lanham, MD: Hamilton Books.

Snyder, G. H. (1984, July). The security Dilemma in alliance politics. *World Politics*, *36*(4), 461–494. doi:10.2307/2010183

Wagner, R. H. (2007). *War and the state: The theory of international politics* (pp. 105–129). Ann Arbor: University of Michigan Press.

Waltz, K. N. (1973). The meaning of anarchy. In R. J. Art & R. Jervis (Eds.), *International politics anarchy, force, imperialism* (pp. 10–20). Boston, MA: Little, Brown and Company.

White, S. P. (2018). Understanding cyberwarfare: Lessons from the Russia-Georgia war. *Modern War Institute – West Point 20, March, MWI Report*. Retrieved from https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf