LAST CALL FROM A SURVIVOR

Robert D. Hogue*

INTRODUCTION

I have had the great privilege of serving *behind the curtain* at the top of a military Service for almost two decades. The nation has been at war for nearly this entire time. As Counsel for six Commandants of the Marine Corps, I had the opportunity to support and advise the highest levels of the defense establishment as the nation prepared for and prosecuted the War on Terror. On September 11,

*The views and opinions presented herein are those of the author and do not necessarily represent the views of Dep't of Defense ("DoD") or its Components. Appearance of, or reference to, any commercial products or services does not constitute DoD endorsement of those products or services. The appearance of external hyperlinks does not constitute DoD endorsement of the linked websites, or the information, products or services therein.

The author gratefully acknowledges the editorial assistance of Samantha J. Hogue, Esq., and the staff of the National Security Law Journal.

2001, I was the Deputy Counsel for the Commandant, completing my first year of service as a civilian senior executive. In many ways, my journey begins there. On that day, hijackers flew American Airlines flight 77 into the western wall of the Pentagon directly beneath my office, murdering 185 people and injuring many others, myself included. Thousands more were killed and injured in New York and Pennsylvania. No discussion can be held without acknowledging those we lost, and those who, for years, stepped forward to serve our country, in and out of uniform, in a war that would stretch on longer than any in our history.

The attacks on that day drove choices for my family and me that have kept me serving with the Marines.[1] Those choices afforded me the rare opportunity to practice my profession at a very high level in support of a challenging and complex client, during a time of war. Importantly, I had the opportunity to support our wounded and work with young Marines and their families. The twentieth anniversary of September 11 presents an opportunity to reflect on how the attacks affected us and the important changes that occurred in the intervening years. This Article attempts to identify some of the significant threats that have evolved since September 11, and their present and potential future risks. While each threat is important individually, the cumulative effects are greater than the sum, and if left unaddressed, they may create a new gestalt of national risk. Further, this Article intends to reflect on national security matters that can still be affected positively by our society without extraordinary government action, like military intervention, which can be addressed using only willpower and common sense. In sum, the national security issues identified in this Article will require the efforts of future lawyers, policymakers, and pragmatists in the U.S. national security apparatus and the society writ large.

I. IT IS TIME TO RECALIBRATE OUR PRIORITIES – THE NATIONAL DEBT

We have not resolved a clear national strategy for dealing with asymmetric warfare. Although we are better at identifying and

[1] Civilians serve with the Corps; members serve in it.

reducing terrorist threats of the kind posed by the 9/11 attackers, we have arguably been slow to evolve away from our organizing principles—nineteenth-century ideas perfected for the great wars of the twentieth century.[2] We obviously want a mismatch on the battlefield to ensure a decisive win over any enemy, but the very nature of asymmetry dictates that forces will be mismatched; the enemy pursues asymmetric options because he recognizes he cannot win head-to-head battles. The smaller or weaker force seeks the advantage in areas that the United States and its allies do not necessarily recognize as legitimate martial objectives, like terrorizing the civilian population.[3] It pursues a strategy of imposing costs that the dominant force—and the society that supports it—may be unwilling to bear.

The twenty-first-century conflicts in the Middle East and Asia clarify that even a pre-modern society[4] can harm us simply by bleeding us financially. Destabilizing our economy was reportedly an objective of Osama bin Laden ("bin Laden") himself.[5] Related or not the country has experienced significant economic problems, vacillating between prosperity and peril since the beginning of the war in Afghanistan. The country was recovering from the bursting of the tech stock bubble in

---

[2] For purposes of this Article, "organizing principles" excludes tactical and strategy developments such as the increased use of technically advanced systems like satellites, drones and cyber, generally included in the Obama administration's concept of "Light Footprint Warfare." *See* David E. Sanger, *Global Crises Put Obama's Strategy of Caution to the Test*, N.Y. TIMES (Mar. 16, 2014), https://www.nytimes.com/2014/03/17/world/obamas-policy-is-put-to-the-test-as-crises-challenge-caution.html; *see also* Jack Goldsmith & Matthew Waxman, *The Legal Legacy of Light Footprint Warfare*, THE WASH. Q., Vol. 39, Issue 2, pp. 7-21, (2016).

[3] Asymmetric war is discussed in more detail in numerous sources. *See, e.g.*, Benjamin Locks, *Bad Guys Know What Works: Asymmetric Warfare and the Third Offset,* WAR ON THE ROCKS (June 23, 2015), https://warontherocks.com/2015/06/bad-guys-know-what-works-asymmetric-warfare-and-the-third-offset/.

[4] By "pre-modern," I mean a society unlike so-called "first world" societies that are typified by technological advances, financial and social interconnection with other nations, and broad access to modern educational resources, health care, and representative forms of government.

[5] Daveed Gartenstein-Ross, *Bin Laden's 'War of a Thousand Cuts' Will Live On*, THE ATLANTIC (May 31, 2011), https://www.theatlantic.com/international/archive/2011/05/bin-ladens-war-of-a-thousand-cuts-will-live-on/238228/.

the year 2000 when the attacks of September 11 occurred. The recession that followed was succeeded by a recovery, then by The Great Recession of 2008, massive unemployment, followed by full employment, a pandemic, more unemployment, then the recovery we are experiencing at this writing. Above all, the defining domestic feature of this era is runaway debt. It seems bin Laden recognized a weakness that we did not see in ourselves: the inability to forge a consensus around national priorities and make resourcing tradeoffs that reflect them.

After September 11, 2001, we began spending massively as we moved to a wartime footing, expanded the national security enterprise, and began developing technologies and services to acquire intelligence on the new threats as well as the tools to respond both on and away from the battlefield.[6] While these choices may have addressed near-term security weaknesses, they also added to the long-term burden of the national debt, increased drag on the economy, and edged us closer to economic insecurity and a host of vulnerabilities that will follow. Further, this drag has been exacerbated because the country was simultaneously losing a historic economic engine—broad-based, manufacturing-driven prosperity.[7]

This is not an argument against increasing our ability to respond to emergencies or the threats that cause them. Rather, it is an effort to pose a question that does not seem to have been asked: when is long-term debt a good solution for near-term security? Government spending on additional first responders seemed wise in the aftermath

[6] Much has been written elsewhere about the surveillance society. *See, e.g.*, Adam L. Penenberg, *The Surveillance Society*, WIRED (Dec. 1, 2001), https://www.wired.com/2001/12/surveillance/; *see also* David Von Drehle, *The Surveillance Society*, TIME (Aug. 1, 2013), https://nation.time.com/2013/08/01/the-surveillance-society/. For a detailed discussion of the growth of the security state, *see generally* Dana Priest & William M. Arkin, TOP SECRET AMERICA THE RISE OF THE NEW AMERICAN SECURITY STATE, 99-–100, 158, 181 (2011) (describing the explosive growth of highly classified work related to counterterrorism, homeland security, and intelligence, including 850,000 holders of "top secret clearances," 250,000 contractors, and 1200 government organizations at 10,000 locations).

[7] Economic insecurity in this sense does not refer to a business cycle, but to the long-term health of the economy.

of September 11 and undoubtedly *promoted the general welfare*.[8] Additional response capacity assures of our ability to react in emergencies and certainly makes the average citizen *feel* more secure—a legitimate national objective.

Yet, while we focused on the physical aspects of the asymmetric threat at home and abroad, old rivals gained strength economically and militarily around the globe, returning us to strategic competition. These are competitors in the real sense, who are or soon will be military or economic peers of the United States. The expense of maintaining a large military to counter this threat is significant.[9] The additional costs of expanding our military capabilities to ensure we have sufficient offensive power to win in direct conflicts, as well as those required to protect and maintain our 'domestic tranquility,'[10] are steep. But the dollars needed to invest in these capabilities are also required to address other public needs. The requirement arises at a time when some of our economic strength is waning. The public no longer seems to understand, nor demand leadership demonstrate an understanding that public priorities compete for limited public resources.[11] The unconstrained spending of tax dollars not yet

[8] *See* U.S. CONST. pmbl.

[9] "The most recent figures for the gross domestic product suggest that the federal government -- especially military and security -- is growing bigger and faster than at almost any point in history." Mark Trahant, *As in Vietnam Era, Question of Guns and Butter Must be Considered*, SEATTLE POST INTELLIGENCER (Aug. 2, 2003), https://www.seattlepi.com/news/article/As-in-Vietnam-era-question-of-guns-and-butter-1120783.php

[10] *Id.*

[11] Professor Irving Bernstein discussed the cycle of domestic investment via progressive legislation cut short by war in "Guns or Butter: The Presidency of Lyndon Johnson." Wilson's New Freedom statutes were enacted between 1913 and 1915, Roosevelt's New Deal program between 1933 and 1935, and Johnson's Great Society legislation between 1964 and 1966. They shared several important characteristics: a strong and energetic Democratic President who did not hesitate to lead; large Democratic majorities in both houses of Congress, which followed their President; solid public support; and the guns-or-butter dilemma which eventually led the President to abandon domestic reform and lead the nation into war— Wilson into World War I, Roosevelt into World War II, and Johnson into the Vietnam War. IRVING BERNSTEIN, GUNS OR BUTTER: THE PRESIDENCY OF LYNDON JOHNSON (1996).

received adds to the national debt, which at present is growing out of control, as discussed below.

One could argue that some of these problems were not caused by 9/11 and should not be raised in this context. However, expenditures associated with our recovery and response to 9/11 were in many instances designed to place the United States on a war footing. Vulnerabilities at home led to significant investments in defense and security measures that likely would not otherwise have been undertaken. Significant additional debt was and is being incurred to pay the cost. Indeed, the War on Terror has been estimated by one group to cost as much as $6.4 trillion.[12] The attacks changed the economic dynamic in this country, accelerating our transition to a service economy, in part through deepening investment in security-related services like first responders and the military.[13] The point is not to question the value or necessity of these investments but to point out that these are expenses, not investments; they appear not to have competed rationally with other expenditures on the national priority list. We opted to have both guns *and* butter and have taken no steps to protect ourselves from the predictable consequences, which will soon be very real.

David Walker, the former Comptroller General of the United States, has been calling attention to the debt problem for nearly two decades. In a speech at the U.S. Naval Academy in 2006,[14] he predicted that unless significant changes occur soon, America might look very different in the future. "[W]e face unprecedented fiscal risks in the years ahead. The facts on this aren't in dispute. If we stay on our

[12] NETA C. CRAWFORD, UNITED STATES BUDGETARY COSTS AND OBLIGATIONS OF POST-9/11 WARS THROUGH FY2020: $6.4 TRILLION, (2019), https://watson.brown.edu/costsofwar/files/cow/imce/papers/2019/US%20Budgetary%20Costs%20of%20Wars%20November%202019.pdf.

[13] For a detailed discussion of the growth of the security state, *see generally*, DANA PRIEST & WILLIAM ARKIN, TOP SECRET AMERICA, THE RISE OF THE NEW AMERICAN SECURITY STATE (2011) (describing the explosive growth of highly classified work related to counterterrorism, homeland security, and intelligence, including 850,000 holders of top-secret clearances, 250,000 contractors, and 1200 government organizations at 10,000 locations).

[14] David Walker, U.S. Comptroller Gen., Speech before the U.S. Naval Academy, (Mar. 8, 2007).

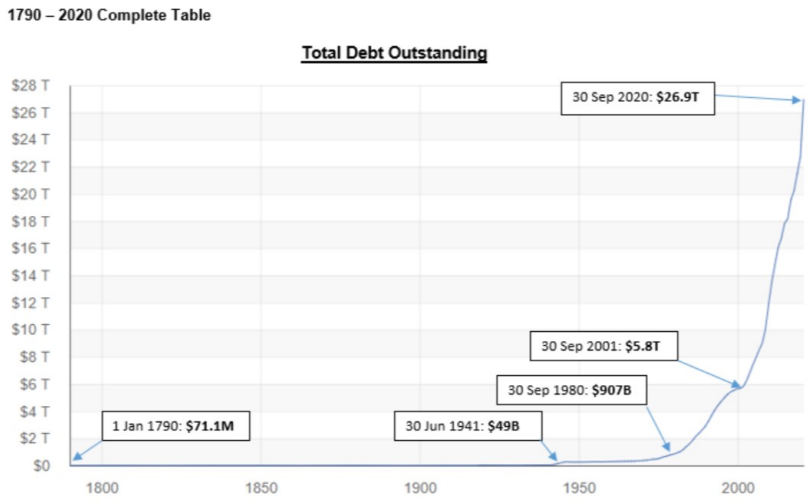
present path, the United States faces a prolonged period of debt and decline."[15] Projecting the long-term consequences of unmanaged debt, he offered the following:

> Back in 1966, discretionary spending, which includes defense, represented two-thirds of federal spending. [In 2006], it was 38 percent and declining. In 1966, defense represented 43 percent of the total federal spending. [In 2006] it was 20 percent, including the current costs for our operations in Iraq and Afghanistan.
>
> Long-range simulations from . . . the U.S. Government Accountability Office (GAO), are chilling. Just six years ago, we were on a path of fiscal sustainability for well over 40 years. Today, based on reasonable assumptions, GAO's simulation model suggests that we will face major economic challenges well before that time. In fact, the simulation model crashes in a little over 40 years.[16]

Today, a mere fifteen years after that projection, the overall numbers are worse. The following graph shows U.S. debt levels starting from the beginning of the Republic. It reveals the staggering growth of U.S. borrowing, particularly since the end of fiscal year 1980. At that time, the national debt was $907 billion.[17] At the conclusion of fiscal year 2001, twenty-one years later, the national debt totaled $5.8 trillion dollars.[18] It took the country approximately 205 years to reach the $5 trillion debt mark (September 30, 1995).[19] It took only thirteen more years to reach the $10 trillion mark at the conclusion of the fiscal year 2008.[20] The next $10 trillion in debt accumulated in just nine years (September 30, 2017).[21] The final $6.7 trillion was incurred in only three years (September 30, 2020).[22] In other words, in the last two

[15] *Id.*
[16] *Id.*
[17] *Historical Debt Outstanding*, FISCAL DATA (last visited July 6, 2021), https://fiscaldata.treasury.gov/datasets/historical-debt-outstanding/.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

decades, the country has incurred five times the debt accumulated in the preceding 200 years.



Source: U.S. Treasury Historical Debt dataset.[23]

If unaddressed, the long-term impact of the uncontrolled national debt will be to limit the government's ability to make public policy choices, and will lead to higher interest payments, tax increases, spending cuts, greater risk of future financial crises, and a general decrease in the nation's ability to respond to crises.[24] More specifically, as noted by the Congressional Budget Office ("CBO"),

> Growth in the nation's debt would dampen economic output over time, and higher interest costs would increase payments to foreign debt holders and thus reduce the income of U.S. households by rising amounts . . . [and] pose significant risks to the fiscal and economic outlook, although those risks are not currently apparent in financial markets. In addition, high debt might cause policymakers to feel constrained from implementing deficit-financed fiscal policy to respond to

[23] *Historical Debt Outstanding*, FISCAL DATA (last visited July 6, 2021), https://fiscaldata.treasury.gov/datasets/historical-debt-outstanding/.
[24] *See generally The 2021 Long Term Budget Outlook*, CONG. BUDGET OFF. (Mar. 4, 2021), https://www.cbo.gov/publication/56977.

> unforeseen events or for other purposes, such as to promote economic activity or strengthen national defense . . . [h]igh and rising federal debt increases the likelihood of a fiscal crisis because it erodes investors' confidence in the government's fiscal position and could result in a sharp reduction in their valuation of Treasury securities, which would drive up interest rates on federal debt because investors would demand higher yields to purchase Treasury securities.[25]

Today, fifteen years after David Walker's clarion call, the CBO's latest long-term budget outlook reflects this debt projection in predicting continuing growth of U.S. public debt out to 2051

> By the end of fiscal year 2021 [September 30, 2021], federal debt held by the public is projected to equal 102 percent of gross domestic product (GDP). If current laws governing taxes and spending generally remained unchanged, debt would persist near that level through 2028 before rising further. By 2031, debt would equal 107 percent of GDP, its highest level in the nation's history, the Congressional Budget Office projects.
>
> Debt would continue to increase thereafter, exceeding 200 percent of GDP by 2051 . . . That amount of debt would be the highest by far in the nation's history, and it would be on track to increase further.[26]

Behind all this debt lurks one of the great challenges of our age, constituting one of the single most significant emerging threats since September 11: curbing the United States' unconstrained appetite. Anything that limits the nation's ability to respond to crises qualifies as a threat to national security. Further, national security encompasses the economic well-being of the country and the prosperity it affords ordinary Americans. Addressing the question of debt is a clear national security priority, acknowledged by Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff, who told audiences in 2010 that "[t]he most significant threat to our national

[25] *Federal Debt: A Primer*, U.S. CONG. BUDGET OFF., (Mar. 12, 2020).
[26] *The 2021 Long Term Budget Outlook, supra* note 24.

security is our debt."[27] He added, "[t]hat's why it's so important that the economy move in the right direction, because the strength and the support and the resources that our military uses are directly related to the health of our economy over time."[28]

It is past time to have a serious public conversation at the national level about the risks associated with borrowing today against future receipts, and this needs to happen outside of political campaigns. Similarly, while the United States must do everything feasible to respond to and prevent future attacks, it also needs a rational public discussion about facing asymmetric threats. The United States needs to find responses that do not require borrowing trillions of dollars to fight asymmetry in pre-modern countries. Our current experience in Afghanistan suggests that the time to assist friendly governments is before showing up with troops; building them after the troops are on the ground risks branding any government that follows as a U.S. pawn. As suggested by Admiral Mullen, we need to recognize that we cannot fight any enemy for long without a strong economy. We need to review the way we spend borrowed dollars to ensure we are not just digging a hole but making investment choices and facilitating economic growth where we can. We need to have the courage to walk away from popular spending programs when other needs present higher, sometimes existential, priorities. Public office holders must recognize that the debt we incur today will saddle our country's children and grandchildren with paying the bills. Further, our inability to make choices between competing national priorities will limit the choices available to our children and leave them vulnerable to our enemies. The United States must adopt resourcing methods that force an evaluation of continuous spending and eliminate the expectation that programs will continue unabated. The consistent use of sunset provisions could help here. Sunset provisions cause publicly funded programs to expire on a specific date unless reauthorized for another specified operational period. Under this mechanism, projects and programs expire by operation of law, avoiding the need to gather support for trying to kill them—an act of

[27] CNN Wire Staff, *Mullen: Debt is Top National Security Threat* (Aug. 27, 2010) (quoting Chairman of the Joint Chiefs of Staff Adm. Michael Mullen) https://www.cnn.com/2010/US/08/27/debt.security.mullen/.
[28] *Id.*

will not often mustered in the current political environment.[29] Failure to do this forces reliance on the flawed assumption that we can even have such a discussion, an issue discussed further below. The long-term effect of rising debt compounds the danger of other problems by limiting resource choices and therefore options for future leaders.

Ultimately, one must ask what victory actually looks like. My hope is that we are learning that whatever else it may be, victory cannot rest solely on expensive, large, national programs or a massive, standing military. I am not a military man, but I am a citizen, and I do not want to see our servicemen and women or our national resources risked unnecessarily. Nor do I think there is an easy answer. Faced with an asymmetric threat, I believe we should be asking ourselves whether mobilizing as if for a World War is the best approach. There are other areas in which we currently hold asymmetric advantages that could be brought into play. We already use economic sanctions to punish bad behavior on the international level; I wonder if we could not harness the great compassion of the American people to expand education and health care capacity in some of the third world places where we are currently killing people, and in the process, undercut the sawdust Caesars who have become strongmen there. Targeted foreign aid would be an inherently less expensive way of deterring future asymmetric threats compared to the trillions of U.S. dollars spent during the last two decades of military interventions. Such alternatives need to be considered to provide an opportunity for the United States to reinvest in itself and further our ability to pay the country's debt. If we do not get our appetite for debt under control, we will one day find that our discretion to spend on the things needed to support our society will be limited by our need to service our debt. When it all

[29] Arguably, the annual appropriations process provides an analog. Simplistically, Congress provides appropriations for authorized programs each year. However, the authorization and appropriations processes are separate; in fact, Rule XXI of the Rules of the House of Representatives prohibits the amendment of existing legislation (including authorizing legislation) through appropriations legislation. *See* Rules of the H.R., 116th Cong., Rule XXI (2019), https://rules.house.gov/sites/democrats.rules.house.gov/files/documents/116-House-Rules-Clerk.pdf. This separation provides a measure of control over appropriations, but to a degree allows authorizers to pressurize the process by creating programs and forcing appropriators to impose fiscal discipline on them, rather than having the full Congress routinely debate each program's merit.

comes crashing down, the white stone buildings on the national mall will be the gravestones of our democracy. On this score, bin Laden can still win.

II. STRATEGIC COMPETITION

While we have been focused on small wars, strategic competition has returned, and with a new twist: our competitors on the global stage are engaging in new forms of warfare made available only in the last few decades, and they are having an effect.

A. Cyber Espionage

China is on a mission to displace the United States as the world's largest economy, and in the process is evolving into a global military power.[30] On the surface, China ostensibly seeks to compete with the United States head-to-head, building its economic capacity at home and its influence abroad. In reality, China seeks not only its own ascent, but the descent of American hegemony. It is implementing bin Laden's strategy of seeking a military advantage through the destabilization of our economy and the erosion of the United States' influence around the world.[31] Some of its methods are easy to spot and understand, some less so.

The growing global connectedness made possible by the internet has opened pathways of exploitation not previously possible. For years, organizations tied to the Chinese government have been

---

[30] "Two decades later, the PLA's objective is to become a "world-class" military by the end of 2049—a goal first announced by General Secretary Xi Jinping in 2017." *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, OFF. OF THE SEC'Y OF DEFENSE, at I (2020), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF [hereinafter *Military and Security Developments*].

[31] *See Annual Threat Assessment of the Intelligence Community*, OFF. OF THE DIR. OF NAT'L INTEL. 6 (Apr. 9, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. "Beijing is increasingly combining its growing military power with its economic, technological, and diplomatic clout to preserve the CCP, secure what it views as its territory and regional preeminence, and pursue international cooperation at Washington's expense." *Id.*

engaging in clandestine cyber and other operations aimed at stealing the intellectual property of American industry as a means of leveling up, both militarily and economically.[32] China's industries do not enjoy the freedom to take the kinds of risks American firms can, and so their ingenuity arguably remains largely untapped. Meanwhile, American firms are both free to experiment and encouraged to do so because they are assured of the rewards brought by owning their intellectual property. Individual expression and the creativity it releases are rewarded in the United States, which provides an environment where business is incentivized to envision the future and to pursue research and development to create it. This will always be an advantage of open societies with 'rule of law' legal systems. But China, at its core, is still a communist system that does not reward personal risk and ingenuity. Communist systems value control by, and prosperity for, a small group of party officials. Those officials have adopted (or at the very least accepted) cyber theft as a state-sponsored supplement to its research and development programs, intended to modernize China and enable it to legitimately compete with American industry.[33] Theft is a tool the Chinese government applies (or sanctions) to achieve its geopolitical objectives.[34]

---

[32] DOD's most recent Report on Chinese military and security developments notes that "[m]ultiple U.S. criminal indictments since 2015 involve PRC nationals, naturalized U.S. citizens or permanent resident aliens from the PRC, and U.S. citizens, procuring and exporting controlled items to China, according to a U.S. Department of Justice summary of major U.S. export enforcement, economic espionage, and sanctions-related criminal cases." *Military and Security Developments, supra* note 30.

[33] The Commission on the Theft of American Intellectual Property, *The Report of the Commission on the Theft of American Intellectual Property*, THE NAT'L BUREAU OF ASIAN RSCH. (2013), https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf ("China has been the principal focus of U.S. intellectual property rights (IPR) policy for many years. As its economy developed, China built a sophisticated body of law that includes IPR protection. It has a vibrant, although flawed, patent system. For a variety of historical reasons, however, as well as because of economic and commercial practices and official policies aimed to favor Chinese entities and spur economic growth and technological advancement, China is the world's largest source of IP theft.").

[34] Christopher Wray, *The Threat Posed by the Chinese Government and Chinese Communist Party to the Economic and National Security of the United States*, FBI (July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-

> A core component of China's successful growth strategy is acquiring science and technology. It does this in part by legal means—imports, foreign domestic investment, licensing, and joint ventures—but also by means that are illegal. National industrial policy goals in China encourage IP theft, and an extraordinary number of Chinese in business and government entities are engaged in this practice.[35]

The United States has aggressively pursued prosecutions for cyber theft, even expanding its efforts to include agents of the Chinese government, but with seemingly little or no effect. Take the following three examples:

In 2014, in the first ever indictment of its kind, five Chinese military officers were indicted on charges of cyber espionage.[36] The defendants were alleged to have conspired to hack into U.S. entities, access their computers, and steal information that was useful to their competitors in China, including state-owned enterprises.[37] In some cases, the conspirators were alleged to have stolen sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the U.S. entity.[38]

In October 2018, a group of China's Ministry of State Security ("MSS") intelligence officers, associated cyber actors, and other co-conspirators were indicted on charges of conspiring to steal sensitive

---

security-of-the-united-states ("[China is] waging this fight not through legitimate innovation, not through fair and lawful competition, and not by giving their citizens the freedom of thought and speech and creativity that we treasure here in the United States. Instead, China is engaged in a whole-of-state effort to become the world's only superpower by any means necessary.").

[35] The Commission on the Theft of American Intellectual Property, *supra* note 33, at 3.

[36] *See U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, DEP'T OF JUSTICE (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [hereinafter *Press Release*]; *see also* Devlin Barrett & Siobhan Gorman, *U.S. Charges Five in Chinese Military of Hacking*, THE WALL ST. J. (May 19, 2014), http://www.wsj.com/articles/SB10001424052702304422704579571604060696532.

[37] *Press Release, supra* note 36.

[38] *Id.*

technological information related to turbofan engines used in commercial airliners.[39] At the time of the intrusions, a PRC state-owned enterprise ("SOE") was also developing a comparable engine for use in commercial aircraft manufactured in China and elsewhere.[40]

In July 2020, two hackers, both nationals and residents of China, were indicted by a federal grand jury in Spokane, Washington, for allegedly hacking into the computer systems of hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the United States and abroad, including Hong Kong and China. The defendants were alleged to have acted, in some instances, for the benefit of the MSS or other Chinese government agencies.[41]

General Keith Alexander, former Director of the National Security Agency, opined in 2012 that American intellectual property was worth about $5 trillion.[42] "Of that, approximately $300 billion [6%] is stolen over the networks per year."[43] He called the theft "the greatest transfer of wealth in history."[44] In 2020, FBI Director Christopher Wray echoed those remarks and added, "the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic

---

[39] *See Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years*, DEP'T OF JUSTICE (Oct. 30, 2018), https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal [hereinafter *Chinese Intelligence*].

[40] *Id.* ("This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking.").

[41] *Two Chinese hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research,* DEP'T OF JUSTICE (July 21, 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion. Additional information on prosecutions related to Chinese espionage is available at https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

[42] Keith B. Alexander, Conference at the Am. Enterprise Inst. (July 9, 2012).

[43] *Id.*

[44] *Id.*

espionage threat from China. It's a threat to our economic security—and by extension, to our national security."[45] He also noted that "the potential economic harm to American businesses and the economy as a whole almost defies calculation."[46]

B. Effect on the American Manufacturing Sector

Indeed, calculating the effects of theft of economically valuable information on this scale is virtually impossible, but there are indicators in the industries targeted by such espionage that reveal a daunting impact on America.

The effects of China's efforts are most obvious in the manufacturing sector, where decades of economic data provide an indication of the effects on American industry. Although the specific effects of espionage cannot be extracted from this data, there is a clear correlation, an inverse relationship, between the rise of Chinese cyber espionage and the rapid decline of manufacturing in America. The manufacturing sector is, in many respects, the 'canary in the coal mine.'

For decades the U.S. manufacturing sector created and supported a middle-class existence for millions of families whose primary wage earners typically lacked higher levels of skill, education, or the resources to enable their pursuit. Such workers, comprising a significant percentage of the U.S. labor force, were nonetheless able to support their families with stable jobs offering good pay and benefits.[47] The manufacturing sector, in all its forms, provided much of that stability. But American manufacturing losses in the twenty-first century have been alarming and are indicative of a larger restructuring

---

[45] Wray, *supra* note 34.

[46] *Id.*

[47] Gary Yakimov & Lindsey Woolsey et al., *Innovation and Product Development in the 21st Century,* HOLLINGS MANUFACTURING EXTENSION PARTNERSHIP ADVISORY BOARD (Feb. 2010), http://www.nist.gov/mep/upload/MEP_advisory_report_4F_24l.pdf. U.S. manufacturing jobs, on average, "pa[id] 9 percent more in wages and benefits than jobs in the overall economy" in 2010. Further, manufacturing workers were becoming more educated and skilled, though 47 percent of U.S. manufacturing workers had not completed education beyond high school.

of the U.S. economy. This economic decay is taking with it the middle-class standard of living that average U.S. manufacturing workers enjoyed for more than a century, and China plays a major role in this decline.

The fading of U.S. manufacturing in the first decade of this century surpassed the Great Depression. In the period 2000 to 2010, the U.S. manufacturing sector lost 5,859,000 jobs.[48] In contrast, manufacturing job losses during the Great Depression, specifically the period measured from the peak of the economic cycle preceding the Great Depression to the employment low point, i.e., 1929 – 1933, totaled 2,766,000.[49] Some writers have argued there is even more to the story.

> [W]hile manufacturing accounted for 43 percent of the jobs lost in the Great Depression, it accounted for 34 percent of all jobs at the time. In [the period 2000-2010], manufacturing accounted for nearly one-third of the job loss even though it represented just one-tenth of the jobs. In other words, in the Great Depression jobs losses were 26 Percent more concentrated in manufacturing compared to the entire economy, while in the [2000s] they were three times more concentrated in manufacturing.[50]

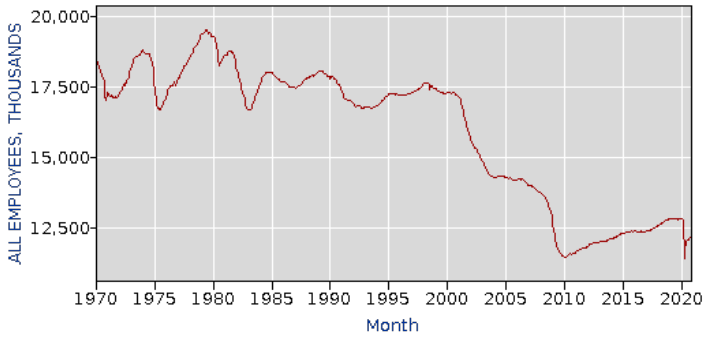
---

[48] U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES, §12,399, Table 620 (2012), https://www.census.gov/library/publications/2011/compendia/statab/131ed/labor-force-employment-earnings.html.

[49] U.S. Census Bureau, STATISTICAL ABSTRACT OF THE UNITED STATES: 1935, §32 at716, Table 756 (1935), https://www.census.gov/library/publications/1935/compendia/statab/57ed.html. For a discussion of limitations on employment data collection at the time of the Great Depression, *see*, John E. Bregger, *The Current Population Survey: a Historical Perspective and BLS' Role*, 107 NO. 6 MONTHLY LABOR REV. 8 (1984).

[50] Robert D. Atkinson et al., *Worse than the Great Depression: What Experts Are Missing About American Manufacturing Decline*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION 6 (2012). The authors further argue that "manufacturing job loss was relatively slow and modest until just the last decade. From 1980 to 1999, manufacturing jobs declined by an average of 0.5 percent per year. But from 2000 to 2011 the rate of loss dramatically accelerated, with manufacturing jobs shrinking at a rate nearly six times faster (3.1 percent per year) than the rate in the prior two decades. Manufacturing lost 5.4 million jobs for a decline of 31.4 percent. (Figures 1

Job losses are dramatically evident in data maintained by the Bureau of Labor Statistics, as represented in the following chart showing manufacturing employment over five decades.



Source: BLS Series ID CES3000000001[51]

While the economy has been restructuring away from manufacturing, the service sector of the U.S. economy has been growing for decades. Although some see these gains as ameliorating the impact on employment,[52] they mask a far more insidious result.

---

and 2) The economy lost 13 times as many manufacturing jobs between 2000 and 2010 than between 1990 and 2000." *Id.* at 5 (citing Bureau of Labor Statistics, *Quarterly Census of Employment and Wages* (private manufacturing establishments, U.S. total, all establishment sizes, 2000, 2011), ftp://ftp.bls.gov/pub/special.requests/cew/beta/.).

[51] U.S. BUREAU OF LAB. STATISTICS, Employment, Hours, and Earnings from the Current Employment Statistics Survey BLS Series ID CES3000000001, https://data.bls.gov/pdq/SurveyOutputServlet (last visited Nov. 1, 2021).

[52] *See* Mack Ott, *The Growing Share of Services in the U.S. Economy—Degeneration or Evolution?,* FED. RSRV. BANK OF ST. LOUIS REV., at 5-22. (June/July 1987), https://doi.org/10.20955/r.69.5-22.bzk. *See also* Corby Garner et al., *Survey of Current Business*, Vol. 100, No. 4, (Apr. 2020), https://apps.bea.gov/scb/2020/04-april/0420-integrated-industry-level-production.htm ("The largest contributors to the aggregate capital input contribution over the period were the finance, insurance, real estate, and rental and leasing sector and the other services sector. *The other services sector itself accounted for over half of the aggregate contribution of labor input.* Taken together, these results quantify the growing importance of services in the U.S. economy. On the other hand, most of the contributions to aggregate [multifactor productivity (MFP)] growth originated in MFP growth within the

Manufacturing sector losses are not being offset by wage-equivalent jobs for less skilled American workers. The lost jobs are generally replaced with lower-paying, less secure service sector jobs, accelerating income inequality.[53] "The service sector now employs more than 85% of the workers in the United States."[54] What remains within the manufacturing sector is also changing, shifting to a higher skill base, making the sector even more inaccessible to the ordinary American worker without special skills.

> Trade and technology have reduced the demand for certain types of work, particularly less-skilled labor in fields like manufacturing . . . the sector now employs only two-thirds as many people as it did 30 years ago. Technological change has widened the wage gap between skill levels. While a man with a high school degree earned about three-quarters of the wages of his college-educated counterpart in 1980, he now earns about half as much. At the same time that technology has made certain jobs obsolete, new jobs are being created in other areas (both high-wage managerial and technical jobs and low-wage service sector jobs), but these new jobs often require different skills or pay lower wages.[55]

---

manufacturing sector (mostly computers and electronic products) and the trade sector." (emphasis added)).

[53] Manufacturing declined approximately 30% between 1970 and 2010. *See* U.S. BUREAU OF LAB. STATISTICS, *supra* note 51.

[54] Alison Felix, *The Growing Importance of the Services Sector*, KANSAS CITY FED (Mar. 29, 2019).

[55] ELEANOR KRAUSE & ISABEL SAWHILL, WHAT WE KNOW AND DON'T KNOW ABOUT DECLINING LABOR FORCE PARTICIPATION: A REVIEW 2 (2017). *Cf.* Bertrand Gruss & Natalija Novta, *The Decline of Manufacturing Jobs: Not Necessarily a Cause for Concern*, IMFBLOG (Apr. 9, 2018), https://blogs.imf.org/2018/04/09/the-decline-in-manufacturing-jobs-not-necessarily-a-cause-for-concern/ (arguing that a shift away from manufacturing jobs need not necessarily be a cause for worry; so long as the right economic policies are in place, growth in the transportation, telecommunications, financial, and business services sectors can offset the effects manufacturing job losses.) *See also* Kerwin Kofi Charles et al., *The Transformation of Manufacturing and the Decline in U.S. Employment* (Nat'l Burea of Econ., Woring Paper No. 24468, 2018) (contending among other things, that the loss of manufacturing jobs has not equated to a decline in manufacturing output. The authors argue that the manufacturing sector evolved into a much more capital-intensive sector during this period, and that its labor force was less likely to be drawn from those with less education. Citing data showing the manufacturing sector's

While some commentators believe that job losses in the manufacturing sector are the result of automation and other technology advancements safeguarding the sector against lost productivity, others have challenged that notion, rejecting the view that the sector is simply becoming more productive.

> [The] . . . dominant view on the loss of manufacturing jobs is fundamentally mistaken. Manufacturing lost jobs because manufacturing lost output, and *it lost output because its ability to compete in global markets—some manipulated by egregious foreign mercantilist policies, others supported by better national competiveness policies, like lower corporate tax rates—declined significantly*. In 2010, 13 of the 19 U.S. manufacturing sectors (employing 55 percent of manufacturing workers) were producing less than they there were in 2000 in terms of inflation-adjusted output. Moreover, . . . the government's official calculation of manufacturing output growth, and by definition productivity, is significantly overstated. Overall, U.S. manufacturing output actually fell by 11 percent during a period when GDP increased by 17 percent. The alarm bells are largely silent for two reasons: government statistics significantly overstate the change in U.S. manufacturing output, and most economists and pundits do not extend their analysis beyond one macro-level number (change in real manufacturing value added relative to GDP). But the conventional wisdom that U.S. manufacturing job loss is simply a result of productivity-driven restructuring (akin to

output was 5 percent higher in 2017 than it was in 2000 despite a loss of 5.5 million jobs during that period, with many of those losses preceding the Great Recession, the authors make the case that the manufacturing sector requires better education and more technical sophistication than in years past. This skills mismatch, according to the authors, contributes to increased unemployment in prime age workers with a high school education or less. The authors note that the manufacturing sector has traditionally been one in which relatively less-educated Americans, especially less-educated men could achieve labor market success; that "[a] s of 1980, over one-third of employed men between the ages of 21 and 55 with a high school degree or less worked in the manufacturing sector." The authors contend that the combination of import competition from China and the increase in capital investment in the manufacturing sector combined to substantially reduce manufacturing labor during the 2000s.)

> how U.S. agriculture lost jobs but is still healthy) is wrong, or at least not the whole story.[56]

In yet another twist exacerbating the disruption in the manufacturing sector (and indicating further the importance of intellectual property to the manufacturing sector), the introduction of modern technology is creating a demand for higher skills. Historically, technological advances in the manufacturing economy had the opposite effect. For example, during the Great Depression, technological advances in manufacturing tended to displace *skilled* workers.

> The varying impact of technological developments by occupation also helps to explain the differing pattern of job loss across gender and age groups. Increased mechanization and the advent of the assembly line permitted substitution of semiskilled workers for skilled workers, which operated to the advantage of women and younger men compared to older men. [T]he proportion of workers in skilled occupations fell from 12.9% to 11.7% between 1930 and 1940, with the entire decrease occurring among men.[57]

Advanced education and training are increasingly becoming gateways (or barriers) to employment for the millions of workers who could not obtain the higher levels of education or skills required to compete for jobs in the evolving manufacturing sector. Those workers are left to seek employment in lower-paying, service sector positions. Government data also confirms that the outlook for job growth expected over this decade is primarily in the low-tech services arena.

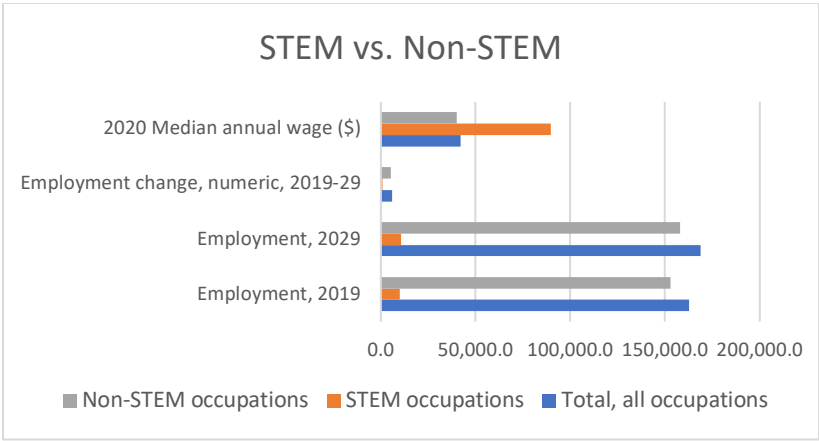
> One of the big problems of the service economy is the quality of jobs. Every month the government announces the quantity of jobs produced but never say [sic] anything about the quality of new jobs. But, if you go to the Bureau of Labor Statistics website and look at Occupations with the Most Job Growth, you will see a 10-year projection of jobs . . . which is 47 million of the fastest-

[56] Atkinson, et al., *supra* note 50, at 3 (emphasis added) (citations omitted).

[57] LINDA LEVINE, CONG. RSCH. SERV., R40655, THE LABOR MARKET DURING THE GREAT DEPRESSION AND THE CURRENT RECESSION 3 (2009) (emphasis added) (citations omitted).

> growing jobs. If you remove the 15 million professional jobs that require a college education or advanced training, you will find that 32 million jobs (68%) have an average wage of $31,561 per year. This is important because 66% of the America's 163 million workers have a high school education or less. The post-industrial service economy is simply not producing enough living wage jobs for workers without college educations.[58]

This shift is dramatically evident in the following chart depicting projected job growth for the period 2019-2029. The chart forecasts that wages for positions in science, technology, engineering and math ("STEM") fields will significantly outpace non-STEM wages, but that non-STEM position opportunities with attendant lower wages dwarf STEM opportunities.[59]



Source: U.S. Dep't of Labor, Bureau of Labor Statistics, Employment Projections, *Occupations with the most Job Growth*, https://www.bls.gov/emp/tables/occupations-most-job-growth.htm.[60]

[58] Michael Collins, *We Must Save America's Manufacturing Sector*, INDUS. WEEK (Nov. 20, 2019), https://www.industryweek.com/leadership/article/22028610/we-must-save-americas-manufacturing-sector. *See also* U.S. DEP'T OF LABOR BUREAU OF LABOR STATISTICS, EMPLOYMENT PROJECTIONS: OCCUPATIONS WITH THE MOST JOB GROWTH (2021).

[59] *Id.*

[60] *Id.*

This confirms that opportunities for less educated, less skilled workers to land jobs paying livable wages are disappearing, and strongly suggests that the middle-class lifestyle is disappearing with them.

What does this have to do with China? These graphs show a correlation between the impact of the ongoing theft of intellectual property from U.S. businesses in order to benefit Chinese manufacturers, and the effects of this knowledge transfer on American industries. However, while the U.S. manufacturing sector was shedding jobs at a rate higher than the Great Depression, China's manufacturing sector was adding them. From 2002 to 2006, Chinese manufacturers, aided by state-sponsored theft, added twelve million jobs.[61] That amount roughly approximates the entirety of employment in the American manufacturing sector at the end of the decade.[62]

The rise of Chinese manufacturing and the parallel growth of its economic influence is an outcome sought by China through legal and illegal means. The decline of U.S. manufacturing and the ensuing effect on the economy is a result equally sought by China. These outcomes do not follow ordinary marketplace competition. The activities that contribute to the disruption of the U.S. manufacturing sector and the displacement of millions of U.S. families are part of a coherent strategy by a foreign power. If conducted by state actors using means other than cyber espionage, these actions might be considered acts of war.

The effects of these developments over decades are now coming clearly into view, and the impacts reach far beyond the dislocation of U.S. workers. In a recent report, the DoD observed that,

---

[61] Erin Lett and Judith Banister, *China's Manufacturing Employment and Compensation Costs: 2002–06*, BLS Monthly Labor Review (April 2009). Additionally, from the end of 2007 to the end 2008, China's total manufacturing employment increased by 1.1 million, from 97.91 million notwithstanding the global economic crisis. Judith Banister & George Cook, *China's Employment and Compensation Costs in Manufacturing through 2008*, BLS Monthly Labor Review (Mar. 2011).

[62] Atkinson, et al., *supra* note 50, at 15.

> [The country should not] ignore Beijing's on-going activities as the world's most egregious cyber threat and intellectual property (IP) thief. America loses nearly $450 billion on an annual basis to cyber hacking, which originates overwhelmingly from China. This behavior already has severely damaged the Department of Defense and its prime contractors, from stolen plans for major weapons systems such as the F-35, to identity theft from America's defense and security workforce.[63]

Cyber espionage must be viewed through a lens that sees more than the loss of the intellectual property; it is an economic bomb. The natural and predictable consequence of our intellectual property losses, as shown above, is the undercutting of U.S. industries (and the U.S. persons employed by them), some of which are critical to the defense of the United States. This became painfully clear as the U.S. mobilized for war after 9/11. For example, when the United States needed to surge production of armored trucks for combat in Iraq in 2007, there was only one steel plant in the nation producing steel of sufficient strength to meet military needs,[64] and that plant had been sold to a European steel firm.[65] Other necessary items were also found to be in short supply, such as oversized tires.[66] "[The] Pentagon had to cobble together an ad hoc network of domestic and foreign suppliers in order to ramp up production of the needed trucks, suggesting that the industrial complex [President Franklin D. Roosevelt] once called 'the arsenal of democracy' had become a rather fragile affair."[67] That alone makes this a national security issue.

Reportedly, the decline of manufacturing in the United States caused the Director of National Intelligence to request a National Intelligence Estimate assessing the nature of the threat.[68] The effects

---

[63] DEP'T OF DEFENSE, FISCAL YEAR 2020 INDUSTRIAL CAPABILITIES REPORT TO CONGRESS 12 (Jan. 2021).
[64] *See* Loren Thompson, *Intelligence Community Fears U.S. Manufacturing Decline*, FORBES (Feb. 14. 2011), https://www.forbes.com/sites/beltway/2011/02/14/intelligence-community-fears-u-s-manufacturing-decline/?sh=72d7fc4186f2.
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*

may prove to be more pronounced than previously recognized. The diminution of manufacturing capacity blunts the United States' ability to respond to significant wartime needs, potentially precluding the type of industrial miracle that carried the United States and its allies to victory in World War II. Worse, this direct impact obscures certain losses that affect the entire defense industrial base, making it particularly significant to national security. Specifically,

> [The manufacturing decline has] had particular impact on the core element of a successful manufacturing economy: the machine tool industry. Of the world's top twenty-one machine-tool makers, only two today are American . . . . By contrast, eight are based in Japan, and six in Germany. And while its domestic machine tool sector remains nascent, China has emerged as a major machine tool customer. Machine tools laid the groundwork for the mobilization miracle of World War II, a fact understood by friends and foes alike, while America has allowed its machine tool sector to turn from a national asset to a national security vulnerability.[69]

In sum, from the economic and national security perspectives, some losses matter more than others. The machine tool sectors provide linchpin products that magnify the capability of manufacturers in other sectors. Losses in such key sectors have cross-cutting harmful effects that can blunt U.S. industrial strength. If the losses in the U.S. manufacturing sector are the 'canary in the coal mine,' the loss of the machine tool sector could represent the beginning of the mine's collapse.

III. CHINA'S PSYCHOLOGICAL WARFARE

September 11 showed us—and the world—that a free people, organized to fight an external threat is a potent force. On September 12, U.S. resolve was palpable. The nation's righteous anger seethed, rumbling and building in its ferocity until it erupted in an explosion of violence in March 2003 as our troops invaded Iraq. For me, the match was lit on the morning of September 12, 2001. I had struggled to get to the Pentagon after receiving a late-night call that the

[69] DEP'T OF DEFENSE, *supra* note 63, at 10.

Commandant wanted to see the senior staff the next morning at 6:00 a.m. I was nursing a brain injury and had lost much of my hearing in the blast. The Pentagon was still on fire and the dead and wounded were still being tallied, but the Navy's operations center had taken a direct hit and the pending bad news hung in the air. In a conference room at the Navy Annex, an anxious and angry crowd of senior officers and executives, enlisted Marines, sailors, and civilians awaited the arrival of the Commandant and the Chief of Naval Operations ("CNO"). They entered the room like a storm. The crowd, suddenly silent, snapped to attention. The CNO strode to the front of the room and slammed a folio onto the table and growled, "I want to know who did this and what we're going to do about it." Even my deaf ears heard the echo of history. It would not be an exaggeration to say that the planning for the war started right then, in that room.

In those moments, faced with an attack on U.S. soil and our blood spilled in our homeland, there was no question that every man and woman in that room would shoulder any burden, bear any cost, or play any part to get into the fight. That unity was a powerful force that swept other crises aside.

Because of that day, we know how much power our collective resolve brings. However, since those early years when we placed ourselves on a war footing and our troops marched, sailed, and flew out to meet our enemies, our unity has crumbled. There are undoubtedly many reasons for this, yet some of the seeds of division were already planted and are growing to full maturity today.

The combination of the loss of manufacturing capacity, the dislocation of millions of workers, and the inability to secure a supply chain for U.S. military needs acts as a risk multiplier. It does more than reduce a significant tax base, accelerating the government toward insolvency. It foments social disruption that can obscure the forces driving these changes, precluding the forging of national unity around issues commonly understood to be national priorities.[70] At least one

[70] One objective of China's three wars is the "[u]ndermining cohesion among an adversary's population by sparking dissension, fostering anti-war elements, and encouraging a feeling of war weariness." *See* Edwin S. Cochran, *China's "Three Warfares": People's Liberation Army Influence Operations*, 20 INT'L BULLETIN OF

author has tied the social component of this phenomenon to effects seen in the electorate:

> This economic disruption has resulted in growing social disruption. While most people in the US assumed the nation was becoming one big middle class, instead a working class facing declining incomes came into clear, angry view during the 2016 US presidential election. The median income of men without a secondary school diploma fell by 20% between 1990 and 2013; for men with secondary school diplomas or some college, median income fell by 13%. The decline of US manufacturing–traditionally a route to the middle class–hit these groups particularly hard. There is now a major income inequality problem.[71]

The descent of these Americans from the middle class has contributed to a growing and corrosive division in U.S. politics, eroding the unity of the country in general. Effective governing of a democracy rests on consensus building. Growing factionalism in the U.S. increasingly challenges our ability to govern ourselves. As the United States becomes more divided, it is less able to identify its national priorities and is therefore precluded from taking coherent action on them. This division weakens U.S. influence in the world and creates openings for its competitors. It is likely for this very reason that China and Russia have injected themselves so substantially into the public discourse in this country.

China, in particular, has overtly adopted a strategic plan that incorporates psychological warfare as one of three types of warfare.[72]

POL. PSYCH. 1, 3, (2020) (citing Dean Cheng, *"Winning Without Fighting: The Chinese Psychological Warfare Challenge"*, HERITAGE FOUNDATION 2 (2013)). China's success under this objective may be seen as the disunion in the United States evidenced in the 2020 presidential election.

[71] William B. Bonvillian, *US Manufacturing Decline and the Rise of New Production Innovation Paradigms*, OECD (2017), https://www.oecd.org/unitedstates/us-manufacturing-decline-and-the-rise-of-new-production-innovation-paradigms.htm.

[72] OFF. OF THE SEC'Y OF DEF., CHINA: THE THREE Warfares 26 (2013) ("In 2003 the Chinese Communist Party (CCP), Central Committee, and the Central Military Commission (CMC) approved the concept of the Three Warfares – a PLA information warfare concept aimed at preconditioning key areas of competition in

"The 'Three Warfares' (san zhong zhanfa or san zhan) concept is a dynamic, nuanced strategic approach to influence operations consisting of three interrelated elements: (1) media warfare (yulun zhan); (2) psychological warfare (xinli zhan); and (3) legal warfare (falüzhan)."[73] Psychological warfare "seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations."[74] In this context, psychological warfare aims to affect the thought-patterns of an opponent's leaders and public.[75] The use of deception is fundamental to this strategy.[76]

> This is supplemented by actively 'implanting doubt and dissent throughout an enemy society while encouraging self-defeating conduct'. China's ancient strategic texts thus teach of deceptive tactics that will enable China to inhibit its opponents from 'fully converting latent into kinetic strength' and thus diminish an opponent's 'power of resistance'.[77]

The demoralizing effect of millions of workers being displaced from the U.S. middle class is consistent with the Chinese strategic approach to warfare and should be assumed to be an intended effect of Chinese economic espionage.

IV. RUSSIA – THE CYBER SABOTEUR

Much has been written about Russia's activities surrounding the 2016 U.S. presidential election. As with China, this Article attempts to show the linkage of these activities to the Russian government as a component of strategic competition, and some of its effects on U.S. targets. China's cyber espionage activities have deep

its favor. The concept is detailed in Chapter 2, Section 18 of the 'Chinese People's Liberation Army Political Work Regulations.'").

[73] Cochran, *supra* note 70, at 3.

[74] OFF. OF THE SEC'Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PRC 2011 26 (2011).

[75] OFF. OF THE SEC'Y OF DEF., *supra* note 72, at 89.

[76] *Id.* at 88; *see also* OFF. OF THE SEC'Y OF DEF., *supra* note 74, at 25 ("In addition to information operations and conventional camouflage, concealment, and denial, the PLA draws from China's historical experience and the traditional role that stratagem and deception have played in Chinese statecraft.").

[77] OFF. OF THE SEC'Y OF DEF., *supra* note 72, at 89 (citations omitted).

roots in its international economic and military ambitions, as discussed above. Russia also has such ambitions but does not seem to have so credible an economic goal. The main focus of Russia's cyber efforts appears to have been destabilization, and while its activities surrounding the 2016 U.S. presidential election have received much attention, less effort has been expended to reveal the confluence of these actions with the prevailing government-sanctioned criminal culture.

The Center for Naval Analysis ("CNA") completed an analysis of Russian cyber operations in September 2016 and concluded that the Russian military conceptualizes cyber operations within the broader framework of information operations, "a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations."[78] CNA noted that:

> Hacktivists and cyber-criminal syndicates have been a central feature of Russian offensive cyber operations, because of the anonymity they afford and the ease with which they can be mobilized. However, the crowd-sourced approach that has typified how the Kremlin has utilized hackers and criminal networks in the past is likely to be replaced by more tailored approaches, with the [Federal Security Services] and other government agencies playing a more central role.[79]

CNA asserts that Russia's view of cyber is different from the Western view.[80] "Russia, more than any other nascent actor on the cyber stage, seemingly devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives."[81] Unlike China's cyber use, Russia's use of cyber appears primarily geared for destructive purposes, at least so far. There is less evidence of economic espionage and less intent to gain an economic advantage by using theft to help build its industrial capability. Based on the available

---

[78] MICHAEL CONNELL & SARAH VOGLER, RUSSIA'S APPROACH TO CYBER WARFARE i (2016).
[79] *Id.*
[80] *Id.* at 2.
[81] *Id.* (*quoting* JAMES J. WIRTZ, CYBER WAR AND STRATEGIC CULTURE: THE RUSSIAN INTEGRATION OF CYBER POWER INTO GRAND STRATEGY 31, in KENNETH GEERS, CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE (2015)).

information, the Russian approach seems dedicated to sowing division and disharmony among its competitors, or to presage or threaten conventional military action.

> In other words, cyber is regarded as a mechanism for enabling the state to dominate the information landscape, which is regarded as a warfare domain in its own right. Ideally, it is to be employed as part of a whole of government effort, along with other, more traditional, weapons of information warfare that would be familiar to any student of Russian or Soviet military doctrine, including disinformation operations, PsyOps, electronic warfare, and political subversion.[82]

According to this view, "information warfare, and by extension cyber, becomes a legitimate tool of the state in peacetime as well as wartime."[83] This view is bolstered by the following quote from General Valery Gerasimov, Chief of the General Staff of the Russian Federation.

> In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template. The experience of military conflicts — including those connected with the so called coloured revolutions in North Africa and the Middle East — confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war.[84]

General Gerasimov effectively describes the emerging use of cyber as a weapon of war. Cyber can be pursued as a separate phase or

---

[82] *Id.* at 3.

[83] *Id.* at 6 (*citing* TIMOTHY L. THOMAS, RUSSIAN INFORMATION WARFARE THEORY: THE CONSEQUENCES OF AUGUST 2008 266 IN STEPHEN J. BLANK & RICHARD WEITZ, THE RUSSIAN MILITARY TODAY AND TOMORROW: ESSAYS IN MEMORY OF MARY FITZGERALD (2010)).

[84] Mark Galeotti, *The 'Gerasimov Doctrine' and Russian Non-Linear War*, IN MOSCOW'S SHADOWS (July 6, 2014), https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

in concert with other phases. Gerasimov also clarifies cyber's utility in the Russian model. It has been said that war is an extension of a nation's foreign policy. Cyber, it seems, is emerging as a new layer of conflict, one in which a cyber actor may act beyond the edge of the policy dimension for the purpose of harming an opponent or competitor—or causing them to hurt themselves—without openly assuming the mantle of the aggressor. In this way, a wide variety of damage may be inflicted, from delegitimizing a government in the eyes of the populace to preventing the delivery of services that the populace needs, or to which it has become accustomed, producing tensions and internal conflict in the victim state. Moreover, the Russians have apparently developed their doctrine and practiced their art for some time.

In April 2007, Russia executed its first "large scale coordinated use of cyber . . . to affect a strategic outcome in a neighboring state,"[85] flooding its websites and internet-based communications infrastructure with pings and data, in what has become known as a "denial of service" attack, effectively halting Estonia's ability to communicate.[86] The attack was effected by Russian-controlled botnets around the world,[87] and followed Estonia's relocation of a prominent World War II memorial to Russian soldiers.[88]

In August 2008, Russia launched cyber-attacks against Georgian government targets, effectively eliminating its ability to communicate during an invasion of South Ossetia by conventional Russian military forces.[89] Similarly, beginning in 2013, Russia appeared to use

> Covert cyber activities in coordination with other information tools and military operations to create a general air of confusion and uncertainty regarding the Ukrainian government's ability to secure its information systems, as well as the integrity of any information being communicated. Through this cyber

[85] Connell & Vogler, *supra* note 78, at 9.
[86] *Id.*
[87] Joshua Davis. "*Hackers Take Down the Most Wired Country in Europe,*" WIRED (Aug. 21, 2007), http://www.wired.com/2007/08/ff-estonia/.
[88] *See* Connell & Vogler, *supra* note 78, at 10.
[89] *Id.* at 12.

> campaign, Russia has been able to quietly and persistently compromise the Ukrainian government and military's ability to communicate and operate, thereby undermining the legitimacy and authority of Ukrainian political and military institutions.[90]

These actions were followed by the Russian invasion and later annexation of the Crimea.

The U.S. Department of Justice ("DOJ") is proceeding with a prosecution strategy that further reveals the Russian government's role in facilitating, or at least permitting these activities. In March 2017, a grand jury in the Northern District of California indicted, among others, two officers of the Russian Federal Security Services ("FSB") in connection with a conspiracy to hack Yahoo's email systems.[91] According to the DOJ, that intrusion resulted in the theft of information from more than 500 million email accounts. According to the indictment,

> The [Federal Security Services] officer defendants, Dmitry Dokuchaev and Igor Sushchin, protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions in the U.S. and elsewhere. In the present case, they worked with co-defendants Alexsey Belan and Karim Baratov to obtain access to the email accounts of thousands of individuals.[92]

The indictment alleges that, using this method, Dokuchaev and Suschin gained access to email and account information of Russian journalists, Russian and U.S. government officials, financial services and equities firms, and others. Dokuchaev and Suschin are alleged to have provided Belan sensitive FSB law enforcement and intelligence information to help him avoid detection by U.S. and other

[90] *Id.* at 14.
[91] Press Release 17-278, Dep. of Just., U.S. Charges Russian FSB Officers and their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017); United States v. Dokuchaev No. 17-103, at 2 (N.D. Cal. Feb. 28, 2017).
[92] *Id.*

law enforcement agencies.[93] Defendant Baratov was arrested in Canada and extradited to the United States, where he pled guilty.[94]

In July 2018, a grand jury in Washington D.C., indicted eleven Russian Main Intelligence Directorate ("GRU") officers, a military intelligence unit (including one also named in a subsequent, October 20, 2018, indictment, listed below) for interference in the 2016 presidential election.[95] The indictment specifies that the defendants

> [K]nowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury (collectively the "Conspirators"), to gain unauthorized access (to "hack") into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.[96]

[93] *Id.*

[94] Baratov's plea is summarized in DOJ Press Release 18-703: In November 2017, Baratov pleaded guilty to Count One and Counts Forty through Forty-Seven of the Indictment. Count One charged Baratov, Dokuchaev, Sushchin and Belan with conspiring to violate the Computer Fraud and Abuse Act by stealing information from protected computers and causing damage to protected computers. Counts Forty through Forty-Seven charged Baratov and Dokuchaev with aggravated identity theft. As part of his plea agreement, Baratov not only admitted to agreeing and attempting to hack at least 80 webmail accounts on behalf of one of his FSB co-conspirators, but also to hacking more than 11,000 webmail accounts in total from in or around 2010 until his March 2017 arrest by Canadian authorities. In addition to any prison sentence, Baratov agreed to pay restitution to his victims, and to pay a fine up to $2,250,000, at$250,000 per count, with any assets he has remaining after satisfying a restitution award.
Press Release 18-703, Dep. of Just., International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison, (May 29, 2018).

[95] Press Release 18-923, Dep. of Just., Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election, (July 13, 2018).

[96] U.S. v. Netyksho, No. 1:18-cr-00215-ABJ, at 2 (D.D.C. Aug. 13, 2018).

In October 2018, a grand jury in the Western District of Pennsylvania indicted six defendants, all officers in the GRU.[97]

> These GRU hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort.[98]

Russia has been developing its doctrine and tactics concerning the use of cyber as a phase of warfare for more than a decade. Given this backdrop, it should not be surprising that in 2016,

> Russian operatives associated with the St. Petersburg-based Internet Research Agency (IRA) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States.
>
> Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election.[99]

Russia is a cyber saboteur; it seeks (1) not so much the advancement of its own narrative as the dissolution of any potential competitor or counter-narrative, and (2) to limit the capacity and

---

[97] Press Release, Dep. of Just., Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (Oct. 4, 2018).
[98] *Id.*
[99] S. REP. NO. 116-XX, at 3 (1985).

support of target states as a precursor to, or as a phase of, conventional military action. Accordingly, its efforts to distract and confuse U.S. voters during the 2016 presidential elections were not surprising; it was both predictable and entirely consistent with its recent history and developing doctrine.

V. TRUTH HAS BECOME A CASUALTY

The attacks of September 11 exposed a cross-cutting set of vulnerabilities touching many facets of our lives, including what most think of in this context—our physical vulnerability. I have resisted writing on this obvious vulnerability angle because I do not want to educate our enemies. Still, it is important to acknowledge that our society's openness, by its very nature, leaves us susceptible to harm. Further, we have adversaries who want to hurt us and are happy to do so by crippling our economy and polluting our political system. Defending in this space is difficult because some of the measures we would have to take to remedy our exposure could alter some of the freedoms we believe important to our society. On this point, I believe we have a vulnerability running much deeper than we imagine, and to my mind, perhaps the most significant vulnerability we carry.

At the turn of the century, we were engulfed in a technological revolution that delivered an explosion of connectedness and capability that disrupted nearly every industry associated with gathering and reporting news and information, including how it was delivered to us. As it turns out, we did not merely accept it; we craved it, despite the fact that it became clear there was little to guide our consumption of it over time. Today, a great mass of information is available to us quite literally at our fingertips. Reams of information once stored in libraries, where it had to be sought out, are now accessed by our cell phones from the comfort of our living rooms. We evolved from the Dewey decimal system to Google searches. Yet we have seemingly little interest in determining the provenance or accuracy of what is delivered to us. Instead, we perfected the harvesting of information for economic purposes. As a result, information is an increasingly well-understood commodity, easily monetized in the digital fora that have sprung up since 9/11.

Entire information systems have arisen, inundating us with data, vying to become our sources of news, information, and, increasingly, thought. The great irony is that from the torrent before us, we fish out only those morsels that support our existing beliefs, shielding ourselves from anything that could upend our convictions. Even when we attempt to search broadly, open to what may come, the social media fora that deliver it to us focus on harvesting and presenting only information they know has some appeal to us. User monitoring tools permit social media companies to study our preferences and use them to draw us to information that they seed with advertising and more data harvesting tools.[100] Inevitably, this has become an unseen force shaping our communion. It is a new form of myopia; we satiate our intellectual curiosity with media tailored specifically for us.[101] The superhighway of the internet is narrowed to a one-lane road leading us to narrow meadows of self-affirming intellectual comfort food.

The effect of this homogenous intellectual diet is that we increasingly believe our own views are the *correct* views; diverse views or thoughts are not sought, nor, increasingly, are they tolerated. Challenging ideas are often presented as threatening. Those who hold different views are shaded as opponents. We allow ourselves to feel justified because we have expended no effort to constrict the free flow of the internet or limit the information it provides. We, therefore, confidently indulge the fantasy that our search results are *in fact* unconstrained. We ignore that the venues we use for news and social

[100] *See generally* Giovanni Luca Ciampaglia &Filippo Menczer, *Misinformation and Biases Infect Social Media, both Intentionally and Accidentally*, THE CONVERSATION (Jan. 10, 2019), https://theconversation.com/misinformation-and-biases-infect-social-media-both-intentionally-and-accidentally-97148 ("The third group of biases arises directly from the algorithms used to determine what people see online. Both social media platforms and search engines employ them. These personalization technologies are designed to select only the most engaging and relevant content for each individual user. But in doing so, it may end up reinforcing the cognitive and social biases of users, thus making them even more vulnerable to manipulation.").

[101] *See* Eli Pariser, *Beware online "filter bubbles"*, TED CONFERENCES (Mar. 2011), https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en (arguing that the personalization of internet services (including news and search results) creates a danger of imposing a "filter bubble" on users, preventing them from being exposed to information that could broaden their experience and understanding).

activity are programmed to attract our attention by increasingly serving up data that interests us. The predictable result is that we no longer believe what we see; instead, we see only what we already believe.

Our willingness to indulge this new myopia is a major vulnerability for several reasons, not least because it affects our ability to address other risks. It not only encourages self-righteous close-mindedness, but it also sandbags our intellect. Our views are apparently objectively confirmed. Consequently, we have no patience for an intelligent discussion about global challenges that may prove existential because views that are either inaccurate or representative of a minority view are presented as unquestionably valid. For example, global warming cannot be addressed so long as science is questioned, and Russian troll farms cannot be exposed if they are unwittingly relied on as a source of news. Without the tools to help us understand what is false or manipulative, we are more likely to hold on to our own views and push back on people or information that challenges them. Because we are targeted individually, each of us can feel justified in accepting what is, in effect, our own personal brand of the truth. This can only lead us to division and conflict—and, as shown above, that is precisely what our adversaries want.

Those who exploit us understand this new vulnerability, where one troll can fan our emotional flames on topics that divide us and cause chaos in our economy, society, and government. They are pouring themselves into it, advancing hidden objectives by disinforming us, and, in the process creating a new asymmetry, disrupting democratic ideas with designer brand false information. This undoubtedly takes numerous forms, but there are two primary expressions of this effort that should be recognized. The first is exploitation at the personal level, best exemplified by identity theft. This is commonly perpetrated through falsified solicitations or credentials in internet communications.[102] The use of false identities

[102] *See generally* UN OFF. ON DRUGS & CRIME, HANDBOOK ON IDENTITY-RELATED CRIME (2011); s*ee also* Jared Thorne & Andy Segal, *Identity Theft: The New Way to Rob a Bank*, CNN (May 22, 2006), http://us.cnn.com/2006/US/05/18/identity.theft/index.html; *see also* NATIONAL

or no identity at all is a hallmark of internet publication,[103] and so far, there is no foolproof way of determining the provenance of information provided on the internet. Accordingly, consumers of internet information remain at risk of being defrauded. Probably every American has heard of or knows someone who has been deceived in this way. This is important because acknowledgment can provide a mechanism for punching through the self-affirming algorithms of social media as we approach the next form.

The second harmful form of disinformation aims at creating national-level effects and was on full display in the 2016 U.S. presidential election, which saw an aggressive Russian disinformation campaign designed to influence American voters to affect the election's outcome.[104] For purposes of this Article, it does not matter who benefited or was hurt by this interference. What matters is that it happened and that it revealed an angle of attack. Our intelligence services are unanimous in this view.[105] Whatever is in our nature that blunts our wariness, allowing us to be deceived on a personal level, also works on the societal level. Its significance is that we are susceptible to foreign (or criminal) interference in our election processes. This strikes a blow at the heart of what it means to be American—our free elections.

Our form of government is founded on the idea that the people pick representatives who will faithfully express their views in the legislative process, empowering it by reflecting the will of the

---

ENDOWMENT FOR DEMOCRACY, *ISSUE BRIEF: HOW DISINFORMATION IMPACTS POLITICS AND PUBLICS* (2018).

[103] The American ideal of free expression is certainly a factor in preserving the internet as a forum for the broadest possible range of ideas, but perhaps the time has come to ask whether free publication must mean responsibility-free publication; whether the right to publish does not carry a corresponding responsibility of provenance and accountability. *Cf.*, *Associated Press v. United States*, 326 U.S. 1, 19-20 (1945) ("[The First] Amendment rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society.").

[104] S. Rep. No. 116-XX, at 32 (1985).

[105] Ken Dilanian, *Intelligence Director Says Agencies Agree on Russian Meddling*, NBC NEWS (July 21, 2017), https://www.nbcnews.com/news/us-news/intelligence-director-says-agencies-agree-russian-meddling-n785481.

majority. Attacks like we saw in 2016 harm us by skewing the pre-election dialogue away from issues that might otherwise dominate the electorate's deliberation. Instead of policy choices affecting the future, the 2016 dialogue became dominated by what we opposed, or more insidiously, it became trapped in a fictitious dialogue about imagined threats to our way of life—as interpreted by each of us individually. The world was portrayed as filled with enemies, threats that needed to be eliminated, a persecution myth that created an urgent sense of peril harnessed by political campaigns to forge and mobilize a base of support. Fear was channeled as a weapon against political opponents. While political scientists may argue that fearmongering is nothing new, never before has this tactic so thoroughly or effectively swayed our elections. What distinguished 2016 is that it was our enemies who fed us this narrative as a means of destabilizing our lives, creating and exacerbating divisions in our culture, preventing the emergence of a majority, and breaking our society down into a polygarchy.[106]

An attack on our election processes ultimately prevents the accurate expression of the will of the people in the governing process. Yet many Americans refuse to accept the reports of electoral interference. One might assume that such refusals are based on a fear that the acceptance of the likelihood of interference in our elections is potentially an admission calling into question the election's legitimacy. Yet, it is also possible that those who reject the expert's conclusions are simply being fed "alternative facts" by those promoting the fraudulent messaging, those convinced by them, or by the social media algorithms that serve up disinformation with impunity. Sadly, this is the level of dialogue in the most advanced democratic society on the planet.[107]

[106] "Polygarchy" is intended to describe a society that is experiencing a significant devolution of its central organizing principles and finding itself balkanized around competing ideas about what the remains of its government is or should be.

[107] The destabilizing effects of disinformation are not limited to developed nations. *See* Conor Sanchez, *Misinformation Is a Threat to Democracy in the Developing World*, COUNCIL ON FOREIGN RELS. (Jan. 29, 2019), https://www.cfr.org/blog/misinformation-threat-democracy-developing-world.

CONCLUSION

We have entered into a period in which we have elected to carry enormous debt. Our ability to pay this debt is hampered by the devolution of economic opportunities for a large percentage of the taxpaying public, an economic disability fueled in part by Chinese espionage. Americans are facing, today, the prospect of incurring enormous debt to hang onto a way of life that the country simply may not be able to afford. Additionally, we face the very real prospect of being overtaken, economically and militarily, by a foreign power. Finally, perhaps the most critical accelerant of all, we are so immobilized by personal and political division that we seemingly cannot have an intelligent public dialogue about addressing these challenges. This immobilization is partly because this country's leaders hyperbolize every facet of the conversation about running the country. It is also partly because China and Russia have infested social and other media to seed our discourse with divisive ideas, fanning the flames to ensure a bonfire of petty hatred, which distracts us from identifying clear national priorities. They promote doubt and distrust as a way of preventing ordinary citizens from accepting or even identifying the truth when shown. As a result, truth has become our greatest casualty—a development that only benefits our enemies.

President Lincoln is reported to have said,

> At what point then is the approach of danger to be expected? I answer, if it ever reach us, it must spring up amongst us. It cannot come from abroad. If destruction be our lot, we must ourselves be its author and finisher. As a nation of freemen, we must live through all time, or die by suicide.[108]

The last few years reveal new truth in this observation. President Lincoln saw that the truest danger to our democracy comes from within, that a free society will always organize to fight external dangers, and that a force of free people will be the most formidable. However, democratic societies are subject to swells of public opinion;

[108] President Abraham Lincoln, Lyceum Address (Jan. 27, 1838).

upheaval may result from faulty information or ideas that spread out of control. Moreover, the strength of will that enables us to forge a society of free people carries with it the risk of hubris. People who are fed self-affirming information may believe they have a deeper understanding of the truth about an important social or political issue, perhaps even to the point where they believe that patriotism requires they take up arms, completing their conversion into the shock troops of a Russian or Chinese troll farm.

American self-determination is based on the right of free expression, a right to which we have become accustomed. Lately, we seem to have become convinced that the right of expression makes our expression right; we equate protest with pursuing paths that could cause our destruction. In the end, we have a right of free speech but an obligation of tolerance. There are multiple troubling examples of our unwillingness to listen to each other while at the same time blindly accepting what is fed to us through the internet. A multi-billion-dollar industry has sprung up around us based on the monetization of sensationalized information, and it is being weaponized in a way that poses a direct threat to our national security and democracy. In this world that we expended blood and treasure to secure, truth itself has become a casualty.

Our country represents the greatest instantiation of "government by the people" in history. How we are governed depends in no small way on what we stand for. We cannot allow ourselves to be seduced by those with political objectives seeking to convince us that we can spend without consequence, in effect bribing us with our own money and the prosperity of our children. Nor should we indulge our xenophobia, spending everything we have to arm ourselves to the teeth to fend off shadowy enemies that we fear may hurt us from great distances using simple tools and tactics. It is time we looked at the dangers closer to home, including those emanating from within. In the days following the September 11 attacks, I borrowed from Lincoln, telling a reporter that I hoped we would find a way to appeal to the better angels of our nature. My hope was that we would not march off in our righteous anger recklessly attacking in all directions, losing ourselves in the process.

That is still my hope.