IN THIS ISSUE

Don't Take Your Base: America's Baseball Diplomacy with Cuba
Nathaniel C. Bader

China-Taiwan Cross-Strait Relations: Evaluating Taiwan's Response to China's Reunification Quest
David Schneider

A Review of the Trump Administration's National Cyber Strategy
Wade H. Atkinson, Jr.

An Evaluation of the Economic Espionage Act 18 U.S. Code § 1831
Michael Eddi

ACTIVE MEASURES

A Student Journal of The Institute of World Politics
Volume V, Summer 2020

ACTIVE MEASURES

Summer 2020 – Volume V

Don't Take Your Base: America's Baseball Diplomacy with Cuba
Nathaniel C. Bader 4

China-Taiwan Cross-Strait Relations: Evaluating Taiwan's Response to China's Reunification Quest
David Schneider 19

A Review of the Trump Administration's National Cyber Strategy
Wade H. Atkinson, Jr. 35

An Evaluation of the Economic Espionage Act 18 U.S. Code § 1831
Michael Eddi 57

ACTIVE MEASURES

Summer 2020 – Volume V

Founding Editors
Daniel Acheson – Michael Webber

Editor-in-Chief
Geoffrey Seroka

Contributing Editors
Jonathan Earles – Kelly Zug

Active Measures *is a not-for-profit scholarly journal published and administered by students of The Institute of World Politics. The views presented in* Active Measures *are those of the authors alone and are not the views of the United States government, The Institute of World Politics, or any other entity.* *All essays published herein are property of their respective authors and are used with permission. All rights reserved.*
Design ©2013 The Institute of World Politics. All rights reserved.
"Active Measures Man" ©2012 Mark Beauchamp. Used with Permission. All rights reserved.
Inquiries should be directed to activemeasures@iwp.edu or:
Active Measures, *c/o The Institute of World Politics*
1521 16th Street NW
Washington, D.C. 20036

Don't Take Your Base: How the Cancelation of the 2018 MLB-FCB Agreement Impacts Prospects for Normalized U.S.-Cuban Relations

Nathaniel C. Bader

Since the 1960s, Cold War tensions between the United States and Cuba have left ordinary Cubans as well as athletes as pawns in an ideological struggle. The common language of baseball has been used as a diplomatic wedge between the two nations. American government laws and corporate MLB policies, however, have created a system where Cuban players must defect from the island, often by working with human traffickers, to play baseball in the United States. The 2018 MLB-FCB deal that would have permitted Cuban ballplayers to play in America was canceled by the Trump administration before it could take effect. This cancelation has negatively affected prospects for normalized relations between the United States and Cuba.

The crack of a bat hitting a ball has long been a familiar sound in New York City as well as Havana. The National League was established in the U.S. in 1876, and the first Cuban league was established only two years later.[1] For the next 80 years, Cuban baseball players freely signed contracts with American teams. Likewise, American players often traveled to Cuba to play in

[1] Peter C. Bjarkman, *Cuba's Baseball Defectors: The Inside Story* (Lanham, MD: Rowman and Littlefield, 2016), xxvi.

the Cuban winter leagues.[2] After the 1959 Cuban Revolution, Fidel Castro banned professional baseball in favor of an amateur system played simply for "the love of the game." Despite being labeled as *traidores al béisbol* or "baseball traitors" by the Castro regime, dozens of Cuban baseball players have defected from the island since 1960 for the chance to compete in America. Players often rely on human traffickers and legal loopholes in order to make their way from Cuba to the United States and the Major Leagues.

During a period of détente in 2014, the Obama administration permitted Major League Baseball (MLB) to negotiate an agreement with the Federación Cubana de Béisbol or Cuban Baseball Federation (FCB) to allow Cuban baseball players to travel to America and play in the Major Leagues without defecting from Cuba. After two years of negotiations, a deal was reached between MLB and the FCB in December 2018.[3] Before the deal could take effect, however, the Trump administration nixed the agreement, leaving Cuban baseball players and MLB stuck in the middle of an ongoing diplomatic struggle characterized by inconsistent government policies toward Cuban migrants and MLB policies that favor human trafficking.[4] This paper will examine past U.S. government and MLB policy, how baseball has been used as a diplomatic tool, why and how players defect, the MLB-FCB deal struck in 2018, and how the Trump administration's invalidation of the deal impacts prospects for normalized relations.

---

[2] Aaron Klein and Jake E. Marcus, "United States-Cuba Normalized Relations and the MLB Influence: The Baseball Coalition Committee," *University of Miami Inter-American Law Review* 47, no. 2 (August 2016): 265, accessed November 2, 2019, https://repository.law.miami.edu/umialr/vol47/iss2/7.

[3] Jeff Passan, "MLB, Cuba Reach Historic Deal to Allow Players to U.S., Hope for Trump Administration Approval," *Yahoo Sports*, December 19, 2018, accessed October 2, 2019, https://sports.yahoo.com/mlb-cuba-reach-historic-deal-allow-players-u-s-hope-trump-administration-approval-205934374.html.

[4] Mark P. Sullivan, *Cuba: U.S. Policy Overview*, Congressional Research Service Report No. IF10045 (Washington, DC: Congressional Research Service, 2019), 1-2, https://fas.org/sgp/crs/row/IF10045.pdf.

U.S. Government Policies

The free flow of Cuban baseball players to and from America effectively ended in 1961 with the establishment of the Cuban Embargo under President John F. Kennedy. Under the Foreign Assistance Act of 1961, Congress authorized the President to "establish and maintain a total embargo upon all trade between the United States and Cuba."[5] The impact of the embargo was felt immediately, as Cuban players could no longer be signed directly out of Cuba. After the Cuban government refused to allow him to return to the U.S. from his native Cuba, Rogelio Álvarez defected from Cuba in 1963 to continue playing with the Washington Senators. Álvarez's defection was the first baseball-related defection to take place under the embargo.[6] Only one other defection would occur in the next twenty-eight years; Bárbaro Garbey, already a successful player on the Cuban national team, defected alongside 125,000 others during the 1980 Mariel Boatlift.[7]

Following the establishment of the embargo, American government regulation and legislation expanded the reach of the sanctions. The Cuban Assets Controls Regulations (CACR), passed by Congress in 1963, broadened the sanctions to include Treasury Department regulation of all commercial activity with Cuba.[8] The goal of CACR was to "isolate the Cuban government economically and deprive it of U.S. dollars."[9] For MLB and its individual teams, CACR meant that agents and scouts could not conduct business in Cuba, which

[5] Foreign Assistance Act of 1961, US Code 2370(a)(2) (1961), § 2, https://www.law.cornell.edu/uscode/text/22/2370.
[6] "Senators Main Concern Is Getting Out Of The Cellar" *Spartanburg Herald*, March 20, 1963, accessed October 5, 2019, https://news.google.com/newspapers?id=QXosAAAAIBAJ&sjid=P8wEAAAAIBAJ&pg=7028,2584936&dq=rogelio+alvarez&hl=en.
[7] Tom Weir, "Cuban Ballplayers Remember Garbey," *USA Today*, July 6, 2005, accessed October 5, 2019, http://usatoday30.usatoday.com/sports/baseball/2005-07-05-garbey-defection_x.htm.
[8] "The US Embargo Against Cuba: Its Impact on Economic and Social Rights," *Amnesty International*, September 2009, accessed October 25, 2019, https://www.amnestyusa.org/pdfs/amr250072009eng.pdf.
[9] Ibid.

eliminated the possibility of Cuban players being identified and signed by American teams while still on the island.

Congressional legislation in the 1990s was aimed at further isolating the Cuban government. The 1992 passing of the Cuban Democracy Act (CDA) further limited the ability of American businesses and their subsidiaries to perform business activities in Cuba.[10] In 1996, U.S.-Cuban relations were further damaged when Cuban MiGs downed two planes belonging to the American charity Brothers to the Rescue or "Hermanos al Rescate."[11] In response, Congress passed the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act, commonly known as the Helms-Burton Act. In addition to placing further restrictions on trade with Cuba, the Helms-Burton Act markedly limited the power of the President to unilaterally ease trade restrictions.[12] The downing of the planes and subsequent passing of the Helms-Burton Act signified the low point of U.S.-Cuban relations in the 1990s.

Baseball Diplomacy and Major League Baseball Policy

In 1999, the Clinton administration began a process of normalizing relations with Cuba. As a part of the normalization of relations, the Department of State authorized the first games in Cuba featuring American teams since 1959.[13] The Baltimore Orioles traveled to Havana in March 1999 to play a series of exhibition games against the Cuban National Team; however,

---

[10] Dianne E. Rennack and Mark P. Sullivan, *Cuba Sanctions: Legislative Restrictions Limiting the Normalization of Relations*, Congressional Research Service Report No. R43888 (Washington, DC: Congressional Research Service, 2018), 1-7, https://fas.org/sgp/crs/row/R43888.pdf.

[11] Elaine de Valle and Manny Garcia and Martin Merzer, "Downed at Cuba's Door: MiGs Blast Two Exile Planes," *Miami Herald*, February 25, 1996, accessed Oct. 17, 2019, https://www.miamiherald.com/news/nation-world/world/americas/cuba/article4556647.html.

[12] Nicole Zaworska, "Striking Out the Cuban Trade Embargo: A Contractual Approach to the Transfer of Cuban Baseball Players to the Big Leagues," *Sports Lawyers* Journal 24, (spring 2017): 138-139, accessed October 17, 2019, https://heinonline.org/HOL/Page?public=true&handle=hein.journals/sportlj24&div=10&start_page=135&collection=journals&set_as_cursor=0&men_tab=srchresults.

[13] Thomas W. Lippman, "U.S. Ready to Play Ball with Cuba," *Washington Post*, January 5, 1999, accessed October 17, 2019, https://www.washingtonpost.com/archive/politics/1999/01/05/us-ready-to-play-ball-with-cuba/4c34b71c-d556-484d-ae8d-da6ae990f7a5/.

policy toward Cuba overshadowed the games themselves.[14] The decision by the Clinton administration to hold games in Cuba provoked various responses from politicians and the baseball community with some claiming the games provided the legitimacy that Castro sought, while others claimed a thawing of relations was praiseworthy.[15] The greatest concern of the games, however, was the question of money. Since the 1960s, American law had prohibited the transfer of funds to the Cuban government. As a workaround, all profits from the games were mandated to go to charities operating in Cuba that were not controlled by the Cuban government.[16] The Cuban National Team traveled to Baltimore in May for another series of games under the same requirements.

The media attention focused on the games highlighted the unique place that sports, particularly baseball, have in capturing and forming public opinion in America.

> *"While Cuban-American exchanges in other professions (orchestra, teachers, etc.) had received some notice, the exchange of baseball teams received wide press coverage. The focus of this coverage was both regarding the respective quality of the teams as well as the potential impact that this type of exchange could have on foreign relations in general. When the games were over, many expected that this type of exchange would continue."*[17]

Despite the hopes of many Americans and the Clinton administration, the Orioles exchange of 1999 was the only such exchange. Republican lawmakers decried the whole series of games as being too friendly to Castro.[18] Orioles Vice-President, Syd Thrift, "lamented to the press that 'the trip was supposed to be non-political. It was supposed to be just

[14] Kupfer Schneider, "Baseball Diplomacy" *Marquette Sports Law* Review 12, no. 1 (February 2001): 475, accessed October 12, 2019, https://scholarship.law.marquette.edu/sportslaw/vol12/iss1/17.
[15] Ibid.
[16] Kupfer Schneider, "Baseball Diplomacy," 474.
[17] Kupfer Schneider, "Baseball Diplomacy," 475.
[18] Kupfer Schneider, "Baseball Diplomacy," 475-476.

baseball.'"[19] Every action between the United States and Cuba, however, involves a political angle. The failure to capitalize on the popular attention paid to the games ultimately thwarted President Clinton's attempts to improve relations with Cuba.

The 1999 Baltimore Orioles trip was not the first time that the U.S. government had used baseball as a diplomatic wedge with Cuba. In the 1970s, then-MLB Commissioner Bowie Kuhn twice attempted to facilitate the playing of exhibition games in Cuba.[20] In 1976, Secretary of State Henry Kissinger authorized the playing of games in Havana, but Cuban involvement in the Angolan Civil War led Kissinger to cancel the games.[21] In early 1977, Kuhn once again reached out to the Cuban government with the proposition for an American all-star team to travel to Cuba to play a Cuban all-star team. The games never occurred because of disagreement between the Cuban Institute of Sports and Commissioner Kuhn about what team would be sent; Fidel Castro wanted to see the Yankees, not an MLB all-star team.[22]

The 1977 debacle left Commissioner Kuhn publicly humiliated and embittered toward Cuba after the proposal fell through in March. One month later, in April 1977, Kuhn sent a letter that came to be known as the Kuhn Directive to all 26 MLB teams.[23] The directive, MLB's first permanent policy toward Cuba, prohibited any Major League club from negotiating with or recruiting any Cuban player.[24] Although U.S. law already restricted the conduct of business in Cuba, including signing contracts with Cuban baseball players, the Kuhn Directive added further restrictions at the corporate level.

---

[19] Peter Schmuck, "O's Won't Pursue Cuban Defectors: Thrift Says Stance is 'Concept,' Not Policy," *Baltimore* Sun, May 18, 2000, quoted in Kupfer Schneider, "Baseball Diplomacy," 476.
[20] Murray Chass, "Behind the Kuhn-Cuba Triangle," *New York Times*, March 12, 1977, accessed Oct. 17, 2019, https://www.nytimes.com/1977/03/12/archives/behind-the-kuhncuba-tangle-the-kuhncuba-tangle-why-trip-fell.html.
[21] Ibid.
[22] Ibid.
[23] Matthew Frankel, "Major League Problems: Baseball's Broken System of Cuban Defection," *Boston College Third World Law Journal* 25, no. 2 (May 2005): 397, accessed October 25, 2019, https://lawdigitalcommons.bc.edu/twlj/vol25/iss2/4/.
[24] Ibid.

After Cuban pitcher Renee Arocha's 1991 defection was facilitated by several sports agents, MLB amended the Kuhn Directive "to forbid all major league teams from discussing and negotiating with anyone in Cuba about signing a Cuban baseball player."[25] "The intersection of MLB guidelines with the Cuban embargo means that any Cuban player seeking to play at the professional level must defect."[26]

Why Cuban Ballplayers Defect

Since Arocha's defection, dozens more Cuban players have defected from the island with the goal of playing professional baseball in the United States. Certain athletes defected due to the poor standard of living in Cuba following the loss of Soviet support in 1990.[27] Still others defected "because the government denied them basic fundamental rights and freedoms."[28] The most common reason for defection, however, is money.

In 1961, Castro dissolved Cuba's professional leagues in favor of a "government-run, amateur system" with wages comparable to that of the common laborer.[29] Since 1961, wages have scarcely risen. Cuban baseball players made around $17 per month in 2013.[30] Recognizing the problem of defection due to money, "the Cuban Baseball Federation more than doubled the $17-a-month wages to $40 in 2014.[31] Bonuses were awarded for the first time in 2013 with, "baseball players who appear in 70 percent of league games [being] awarded $208. League leaders in hitting and other categories get an extra $41. The team that wins the title gets

[25] Kupfer Schneider, "Baseball Diplomacy," 481.
[26] Alyson St. Pierre, "America's Past-time and the Art of Diplomacy," *Indiana Journal of Global Legal Studies* 25, no. 2 (Summer 2018): 805, accessed October 12, 2019, www.jstor.org/stable/10.2979/indjglolegstu.25.2.0797.
[27] Zaworska, "Striking Out the Cuban Trade Embargo," 146.
[28] Ibid.
[29] St. Pierre, "America's Past-time," 801.
[30] Sam Anderson, "Baseball's Last Cuban Escapees," *The New York Times Magazine*, August 20, 2015, accessed Oct. 17, 2019, https://www.nytimes.com/2015/08/23/magazine/baseballs-last-cuban-escapees.html.
[31] Zaworska, "Striking Out the Cuban Trade Embargo," 147.

$2,700 to split."[32] In addition, the Cuban Baseball Federation began allowing its players to compete in foreign leagues such as Japan, Mexico, or Korea in 2014.[33] For Cubans playing baseball overseas, "anywhere from as low as 10% to as high as 75% of the player's overseas salary is paid directly to the Cuban sports arm of the Cuban government."[34] The opportunity to earn more money playing abroad still draws players away from Cuba.

From 2009-2017, Cuban defectors playing in MLB signed more than $330 million worth of contracts with MLB teams.[35] Star players Yasiel Puig and Jose Abreu (both defectors) signed deals worth $42 million and $68 million, respectively.[36] Prior to his defection, Yulieski Gourriel, third baseman of the Cuban National Team and arguably the best player on the island, earned approximately "13,000 Cuban pesos per month ($491 U.S. dollars per month)."[37] Gourriel's yearly salary in Cuba was .0006 percent of the yearly salary of the 5-year, $47.5 million contract that he signed with the Houston Astros.[38]

How Cuban Ballplayers Defect

Defection from Cuba is risky and potentially deadly; up to 75 percent of those who attempted to escape by boat in 1994 died at sea.[39] Some players, such as Renee Arocha in 1991 or

---

[32] "Cuba Lets Athletes Compete in Foreign Leagues…but with a Catch," *New York Daily News*, September 27, 2013, accessed October 17, 2019, https://www.nydailynews.com/sports/cuba-lets-athletes-compete-foreign-leagues-catch-article-1.1469452.

[33] Ibid.

[34] Klein and Marcus, "United States-Cuba Normalized Relations," 274.

[35] Zaworska, "Striking Out the Cuban Trade Embargo," 146.

[36] Klein and Marcus, "United States-Cuba Normalized Relations," 272.

[37] Drew M. Goorabian, "Baseball's Cuban Missile Crisis: How the United States and Major League Baseball Can End Cuban Ballplayer Trafficking,"*UCLA Journal of International Law and Foreign Affairs* 20, no. 2 (Fall 2016): 435, accessed October 14, 2019, https://heinonline.org/HOL/Page?handle=hein.journals/jilfa20&div=16&g_sent=1&casa_token=M0BQOJMSyNcAAAAA:pXRJQoCITFKIu4BCxvWIj6uIOdOhnjHFtPkdmeNESp7OGpV19DXChPF2TfhwvvGxTg3EeTgfID0&collection=journals

[38] "Astros sign Cuban free agent Yulieski Gurriel to 5-year deal," *ESPN*, July 16, 2016, accessed November 2, 2019, https://www.espn.com/mlb/story/_/id/17089767/houston-astros-sign-cuban-free-agent-yulieski-gurriel-5-year-deal.

[39] Zaworska, "Striking Out the Cuban Trade Embargo," 140.

Aroldis Chapman in 2009, defected in relatively safe circumstances while playing for the Cuban National Team in international tournaments.[40] The more common manner of defection is to leave the island and establish residency in another country before signing with an MLB club. Together, MLB rules and U.S. law create differing eligibility and draft requirements regarding players who establish residency in the United States as opposed to those who establish residency in another country.

Under the Cuban Adjustment Act (CAA) of 1966, "Cuban natives or citizens living in the United States who meet certain eligibility requirements to apply to become lawful permanent residents (get a Green Card)."[41] In 1995, the United States began interpreting the CAA to mean any immigrant from Cuba who landed on dry land would be permitted to pursue residency in the United States, while those intercepted at sea would be returned to Cuba.[42] Although many Cubans who defect seek permanent residency in the United States under the CAA, baseball players often do not defect to the United States due to MLB signing procedures for residents of the United States. Cuban players who establish residency in the United States are treated the same as all natural-born or naturalized American or Canadian citizens; thus, Cuban immigrants who establish residency in the United States are subject to the Major League Baseball amateur draft and restrictions on monetary amounts for rookie contracts under MLB rules 3 and 4.[43]

---

[40] Jorge Arangure Jr., "New World of Hope Awaits Chapman," *ESPN*, August 6, 2009, accessed Nov. 2, 2019, https://www.espn.com/mlb/news/story?id=4381376.

[41] "Green Card for a Cuban Native or Citizen," U.S. Citizenship and Immigration Services, August 13, 2019, accessed Nov. 2, 2019, https://www.uscis.gov/greencard/caa.

[42] Elise Labott and Kevin Liptak and Patrick Opperman, "US Ending 'wet foot, dry foot' policy for Cubans," *CNN*, January 13, 2017, accessed Nov. 2, 2019, https://www.cnn.com/2017/01/12/politics/us-to-end-wet-foot-dry-foot-policy-for-cubans/index.html.

[43] Schneider, "Baseball Diplomacy," 480; Walter T. Champion and Danyahel Norris, "Why Not Row to the Bahamas Instead of Miami?: The Conundrum That Awaits Cuban Elite Baseball Players Who Seek Asylum and the Economic Nirvana of Free Agency," *Virginia Sports and Entertainment Law Journal* 9, no. 2 (Spring 2010): 224-225, accessed October 26, 2019, https://heinonline.org/HOL/Page?public=true&handle=hein.journals/virspelj9&div=11&start_page=219&collection=journals&set_as_cursor=3&men_tab=srchresults.

Players who choose to establish residency in a third country avoid contractual restrictions and are free to sign with any team of their choosing. This is known as the "El Duque" model after Cuban defector Orlando "El Duque" Hernandez, who declined asylum in the United States in favor of asylum in Costa Rica. By accepting asylum in Costa Rica, Hernandez signed with the team of his choosing for millions more than he could have signed for if he was a resident of the United States and proceeded through the draft.

The monetary incentives to follow the "El Duque" model may encourage players to seek out "lancheros" or smugglers to ferry them off the island. Yasiel Puig's defection in 2012 was documented in the ESPN investigative report "No One Walks Off The Island."[44] Puig's journey from Cuba to the Majors involved being smuggled to Mexico by the drug cartel "Los Zetas" for $250,000, being kidnapped by a rival cartel, and funneling $8.4 million to the smugglers once he signed his first contract. Jose Abreu paid $6 million to the "lancheros" who helped him escape Cuba in 2013. ESPN's Scott Eden described the trafficking of baseball players by writing:

> *…the smugglers want between 20 percent and 30 percent of the top-line value of a player's first professional contract. That kind of revenue stream has interested a whole lot of colorful people in the underworlds of several countries: Mexico, the Dominican Republic, and, of course, Miami, USA. In Cancun, long the seat of smuggling rings that specialize in bringing regular civilians out of Cuba as well as ballplayers, turf wars have been waged over the business. Players have been stolen at gunpoint from one group by the next, hits taken out, rivals driven by and strafed, bullet-ridden corpses left lying in the streets.*[45]

[44] Scott Eden, "No One Walks Off the Island," *ESPN the Magazine*, April 17, 2014, accessed October 25, 2019, http://www.espn.com/espn/feature/story/_/id/10781144/no-one-walks-island-los-angeles-dodgers-yasiel-puig-journey-cuba.
[45] Ibid.

Any attempts at diplomatic solutions must start with stemming the flow of players via human trafficking and allowing for safer means of coming to the United States to play baseball.

Analysis of 2018 MLB-FCB Agreement

In 2014, President Barack Obama initiated a period of détente with Cuba. The easing of relations was most significantly highlighted by the 2016 visit of Obama to Cuba, where he and Cuban leader Raul Castro enjoyed a baseball game together at Havana's Latinoamericano Stadium.[46] The greatest impact of the "Obama thaw" on baseball was the administration granting MLB a license from the Office of Foreign Assets Control that allowed MLB to negotiate a deal with the FCB that would permit players to sign with MLB teams without defecting from Cuba.[47] In December 2018, MLB and FCB came to an agreement that allowed players over the age of 25 to sign freely with Major League teams.[48] As part of the deal, "[p]layers would come to the United States on work visas, and teams would pay the CBF (FCB)…for the release of their rights."[49] The payment to the FCB would be between 15 percent and 25 percent depending on the age of the player and other factors.[50] MLB has long had similar deals in place with Japan, Korea, and Taiwan.[51] Many sports agents, writers, players, executives, and certain politicians on both sides of the Straits of Florida had long advocated for an agreement that allowed the FCB to preserve its homegrown talent and maintain its own league structure while funneling certain players to the MLB; the 2018 agreement fulfilled those requirements.[52]

---

[46] Claire Felter and Danielle Renwick and Rocio Cara Labrador, "U.S.-Cuban Relations" *Foreign Affairs*, March 7, 2019, accessed Oct. 17, 2019, https://www.cfr.org/backgrounder/us-cuba-relations.
[47] Passan, "MLB, Cuba Reach Historic Deal;" Matt Provenzano, "The MLB-Cuba Posting Agreement is Unambiguously Good Policy," Beyond the Box Score, December 30, 2018, accessed November 2, 2019, https://www.beyondtheboxscore.com/2018/12/30/18160603/mlb-cuba-posting-system-rob-manfred-yasiel-puig-cuba-history.
[48] Passan, "MLB, Cuba Reach Historic Deal."
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Bjarkman, *Cuba's Baseball Defectors,* xxvi.

The Cuban Institute for Sport, INDER, supported the deal and praised its positive impacts on human trafficking by saying in a statement, "The contract will contribute to stopping illegal activities like human trafficking that for years have put the physical integrity and life of many talented young Cuban baseball players at risk."[53] INDER stated the deal would provide a "'collaborative, non-political and stable relationship between the CFB and the MLB" that would guarantee the ability of Cuban players to "be able to play in the American professional Leagues without losing their residency in Cuba or their link to Cuban baseball."'[54] When the deal was announced, sportswriter Matt Provenzano called the deal, "an unambiguously good thing for baseball, for the United States, for Cuba, and the world."[55]

The MLB-FCB deal, however, was not without its detractors. A Trump administration official said the deal "would institutionalize a system by which a Cuban body garnishes the wages of hard-working athletes who simply seek to live and compete in a free society."[56] Florida Senator Marco Rubio called the deal a "farce."[57]

Current players Jose Abreu and Yasiel Puig praised the MLB-FCB deal with Abreu, saying that players, "will be able to keep their earnings as any other player in the world, they will be able to return to Cuba, they will be able to share with their families, and they will be able to play the sport they love against the best players in the world without fear and trepidation."[58] Puig's acknowledgment of the safe pathway the deal created was clear when he stated, "to know future Cuban players will not have to go through what we went through

---

[53] Peter Kornbluh, "Cuba and Major League Baseball Reach Players' Agreement," *Cigar Aficionado*, December 21, 2018, accessed October 2, 2018, https://www.cigaraficionado.com/article/cuba-and-major-league-baseball-reach-players-agreement

[54] Ibid.

[55] Provenzano, "The MLB-Cuba Posting Agreement."

[56] Ibid.

[57] Ibid.

[58] Ibid.

makes me so happy."[59] Major League Baseball spent more than $2 million in 2017 and 2018 lobbying in support of the deal.[60]

Prospects for Normalized Relations

In sharp contrast to the Obama administration's policy of normalizing relations with Cuba, the Trump administration rolled back certain Obama-era efforts to normalize relations, including introducing new sanctions.[61] In 2019, the Trump administration "increased economic sanctions significantly to pressure the Cuban government …[w]ith these actions, U.S. policy toward Cuba has again shifted to a policy of strong economic pressure."[62] In line with the Trump administration's policy of pressure on Cuba, the Department of the Treasury reversed course and nullified the MLB-FCB deal.[63] The Obama administration maintained that the FCB was not a government entity, which allowed for the possibility of monetary transactions between MLB and the FCB. Trump administration officials claimed the opposite and revoked the deal because "the Cuban Baseball Federation is part of the Cuban government and therefore no payments could be made to the federation under U.S. sanctions."[64] This claim is contrary to the Cuban government's statement that the FCB is not a government entity but instead is a subsidiary of the Cuban Olympic Committee, which is a non-governmental entity.[65]

As long as no safe pathway to the United States exists, Cuban baseball players will continue to defect from the island. This process of defection harms the United States on two fronts. First, the inability of defectors to return to the island after being exposed to the capitalist, multi-party system of the United States limits the prospects for democratic reform on the

---

[59] Ibid.
[60] Passan, "MLB, Cuba Reach Historic Deal."
[61] Mark P. Sullivan, *Cuba: U.S. Policy Overview.*
[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Matt Spetalnick, "U.S. Nixes Deal for Major League Baseball to Sign Cuban Players," *Reuters*, April 8, 2019, accessed October 2, 2019, https://www.reuters.com/article/us-cuba-usa-baseball/u-s-nixes-deal-for-major-league-baseball-to-sign-cuban-players-idUSKCN1RK27U.

island. Second, when players defect, they often rely on and pay a large portion of their contract to human traffickers for the chance to play professional baseball in America. With no agreement that allows Cubans to play baseball freely in America, human traffickers will continue to be utilized and paid for the service they provide. An agreement, such as the 2018 MLB-FCB deal, may permit payments to the Cuban government, but it would also significantly reduce the amount of money paid to traffickers. With or without a deal, an entity—criminal smugglers or the Cuban government—will get paid. The United States must decide which option, allowing smugglers to make money from players or permitting payments to the Cuban government, is better aligned with its national interest and values.

The cancelation of the MLB-FCB deal by the Trump administration, along with the repealing of various other Obama-era policies, has placed the United States back in a pre-détente relationship with Cuba and diminished prospects for normalized relations. In order to move beyond a zero-sum, Cold War-style diplomatic relationship with Cuba, baseball diplomacy must be a key aspect of negotiations between the two nations. To begin this process, the United States must develop a clear and cohesive strategy as opposed to the antithetical political policies of diplomatic thaw, which occurred under President Clinton and President Obama, and the increased pressure of President Trump. As evidenced by the slew of legislation regarding Cuba since 1959, Congress has been the primary determiner of American foreign policy toward Cuba, including restricting the power of the executive to unilaterally ease trade restrictions. Since 2000, however, Congress has ceded foreign policy actions regarding Cuba to the executive branch. This devolution of powers has allowed the inconsistent, executive-directed policies that have dictated U.S.-Cuban relations in the 21st century.

In order to move forward, Congress must take a more active role in guiding American foreign policy toward Cuba. The first step in this increased role should be the passage of legislation permitting the 2018 MLB-FCB deal to move forward as agreed

upon, regardless of the status of the FCB. This Congressional action would still allow the primary author of foreign policy, the President, to maintain political and economic pressure or allow for détente with the Cuban government, while simultaneously mandating an olive branch between the two nations. With baseball established as the common language of U.S.-Cuban diplomacy, the two countries may finally be able to "play ball" at the negotiating table.

China-Taiwan Cross-Strait Relations: Evaluating Taiwan's Response to China's Reunification Quest

David Schneider

Reunification with Taiwan has been a top priority for Beijing since the founding of the People's Republic of China (PRC). Recently, President Xi Jinping declared that China will not tolerate the separation of even one inch of its territory. To achieve this goal, Beijing has employed a variety of tactics from enticement to intimidation. This article will examine the shifting patterns of cross-Strait engagement and its impact on Taiwan's stance towards China's goal of reunification, focusing on two case studies.

China has maintained a consistent goal regarding Taiwan since 1979: reunification as "one China" under mainland rule. Beijing's leadership has employed a variety of carrot/stick approaches towards achieving this reality. Taiwan's stance has evolved from its initial one China under a return to Nationalistic KMT rule to an inconsistent pattern under democratic governments, trending more towards economic integration versus sharper restrictions on cross-Strait ties. The Taiwanese population has been caught between motivation to promote economic growth via increased cross-Strait trade and desire to maintain independence from mainland rule in some format.

While Beijing's goal is reunification, the question confronting Chinese leadership has been how best to accomplish this objective. Achieving reunification through peaceful economic and social ties would necessitate persuading the population of Taiwan's blossoming democracy that unification under some form of mainland sovereignty is in their best interest. Cross-Strait economic interdependency has been mutually beneficial but has been imbalanced with China's economy burgeoning in contrast to anemic Taiwanese growth, and with increasing dependency of Taiwan's economy on China.

China has tried to promote positive cross-Strait relations through tourism and by appealing to Taiwan's business community for investment. When that approach has failed to shift attitudes towards reunification, Beijing has employed diplomatic isolation and economic coercion. In addition to its refusal to renounce force as a possible option, the mainland has utilized military tactics designed to intimidate the Taiwanese.

This paper will examine the shifting patterns of cross-Strait engagement and its impact on Taiwan's stance towards China's goal of reunification, focusing on two case studies. While Beijing has explored a potpourri of tactics towards swaying Taiwanese public opinion, it has failed to achieve reunification under PRC sovereignty. Taiwan's support for de jure independence stands at a tiny minority, but convincing the Taiwanese to relinquish some form of sovereignty in the absence of a democratic mainland has proven elusive.

Taiwan's resilience in the face of a dominant adversary provokes the question of what factors underlie the continued resistance to the mainland's model of "one China: two systems." Since 1996 and the initiation of free and direct presidential elections, increasing numbers of Taiwanese identify by their nationality, rather than by ethnic origin. This trend corresponds to the development of a flourishing democracy. The growing sense of Taiwanese national identity, combined with a high value placed on preserving a free and independent democracy, has resulted in the majority of Taiwanese from both major political parties being opposed to reunification under the mainland's terms.

Case Study I: Growing Tensions: the 1996 election and President Lee Teng-hui's third term

The first case illustrates a period when Beijing reacted in a largely bellicose manner to perceived moves by Taiwan towards independence. This study will examine the actions and messaging of the third Lee presidency, and how a series of misinterpretations, as well as fundamental ideological differences, led to increased tension. An assessment of Taiwan's response to China's threats supports the conclusion that the mainland failed to anticipate the Taiwanese people's degree of commitment to their budding democracy and to their growing sense of national identity. Even the more conciliatory gestures extended to the Taishang (Taiwan's business community) failed to bring Beijing's goal into reality.

The election of President Lee Teng-hui in 1996 was a hallmark in Taiwan's political history, as it was the first direct presidential election. Having initially inherited the presidency, Lee embraced democracy and ultimately won the election in 1996 with 54% of the vote. The transition to democracy provoked increased debate on Taiwanese identity and movement away from the "pan-Chinese nationalism" of the previous authoritarian period.[1]

In June 1995, quite possibly as a move to enhance his standing with the Taiwanese electorate, Lee persuaded President Clinton to allow a visit to the United States that included a presentation at his alma mater, Cornell University.[2] [3] [4] This speech proved to be far more political in content than anticipated, and would thus become a critical turning point in Beijing's response.[5] Just two months earlier, Lee had responded to China's call for unification under the Hong Kong model by basing unification on the condition that both sides

[1] Syaru Shirley Lin, *Taiwan's China Dilemma* (Stanford, California: Stanford University Press, 2016), 30.
[2] Ibid, 64.
[3] Murray Scott Tanner, *Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use* (Santa Monica, California: Rand Corporation, 2007), 92.
[4] Richard C. Bush, *Unchartered Strait: The Future of China-Taiwan Relations* (Washington, D.C.: The Brookings Institution, 2013), 14.
[5] Ibid.

endorse a shared commitment to democracy. Previously, Lee had angered Beijing by reaching out to countries that had not established diplomatic relations with Taiwan.[6] [7] When Lee issued his plea for Chinese respect for Taiwanese democratic values, Beijing's negative reaction was about more than Lee visiting his alma mater.[8]

Interpreting Lee's U.S. trip as a trend towards defining Taiwan as a sovereign entity, rather than as a campaign effort to impress domestic voters, Beijing concluded that a tough response was mandated.[9] In the summer of 1995, anticipating legislative elections, and in March 1996 just prior to the presidential election, China conducted a series of military exercises, including missile tests in proximity to Taiwan.[10] [11] Lin attributes this show of force to Beijing's "attempt to discourage voters from supporting pro-independence DPP candidates."[12] By contrast, Bush contends that Beijing was responding to Lee's perceived provocative behavior.[13] While the mainland was certainly opposed to the Democratic Progressive Party's (DPP) pro-independence stance and generally preferred KMT candidates, it also clearly found Lee's views on democracy and separatism, as expressed both at Cornell and previously, highly objectionable. The most plausible explanation is that Beijing was sending a warning to the people of Taiwan to back away from de jure independence or any actions implying a redefinition of its international status.

One important impact of the missile tests on public opinion was a consolidation around Taiwanese national identity. Surveys show that in the period from 1992 to the time of the military exercises in 1995-1996 there was a significant rise in identification as Taiwanese, with a concomitant decline in self-identification as purely Chinese.[14] By exposing the "China

[6] Ibid, 13.
[7] Lin, 53.
[8] Ibid, 64.
[9] Bush, 14.
[10] Ibid.
[11] Lin, 54, 65.
[12] Ibid, 54.
[13] Bush, 14.
[14] Lin, 54-55.

threat," the tests also brought economic and security concerns to the forefront. Mistrust of China's intentions, having been provoked in 1994 after the murder of twenty-four Taiwanese tourists on a lake in Zhejiang, China, was fueled.[15] [16] These events illustrate the vicious downward cycle of mistrust and misunderstanding that often characterized cross-Strait relations.

Another Taiwanese response to the missile tests was a dramatic rise in support for restrictions in cross-Strait economic ties.[17] Although Lee had previously guided Taiwan towards increased engagement with China,[18] he implemented extensive regulations to enable Taipei to track mainland investments and promoted diversification.[19] Based on the "fear that excessive dependence could lead to 'blackmail by Beijing,'" according to Murray Scot Tanner, this approach was formalized as Lee's "Go South" policy in 1994.[20] [21] The list of countries targeted for investment was expanded from ASEAN countries in 1993 to include Central and South America and Africa.[22]

Six months after the last missile test, "Go South" evolved into the "No Haste, Be Patient" policy intended to further crystallize Taiwan's control of funds heading for the mainland. Tanner discusses the link between national security and preventing economic dependency:

> *[Lee] issued a report arguing that as long as Beijing continued its hostility toward Taiwan, unrestrained Taiwan investment in the mainland would undermine national security. The report buttressed its contention with numerous quotes from senior*

[15] Ibid, 64.
[16] G. Van der Wees and Mei-chin Chen, "Fire on the Lake: The Thousand Island Lake Tragedy," *Taiwan Communiqué*, July 1994, International Committee for Human rights in Taiwan, http://www.taiwandc.org/twcom/tc61-int.pdf.
[17] Ibid, 57.
[18] Ibid, 53.
[19] Tanner, 42-43.
[20] Ibid, 43,45.
[21] Lin, 59.
[22] Ibid, 59-60.

> *mainland leaders that called for expanded use of economic ties as a source of political leverage to prevent Taiwan's independence.*[23]

Initially, fear of domination by the mainland corresponded to support for Lee's restrictive policy, although the Taishang hoped that this would be a temporary reaction to the missiles.[24] An additional tool in Beijing's arsenal for thwarting Taiwanese sovereignty has been diplomatic isolation. As Taiwan scholar Bush notes, "Perhaps the political issue that has the greatest significance in the stabilization of cross-Strait relations and beyond is that of Taiwan's participation in the international community, the extent of which is one measure of Taiwan's sovereign status." Bush contends that one element of Beijing's motivation is to reduce Taiwanese "resistance to reunification."[25]

During Lee's second term in office, China blocked Taiwan's participation in the first annual APEC Economic Leaders Meeting in 1993, as well as its bid to join the UN. Beijing's campaign to weaken Taipei's international status also resulted in a reduction of the number of countries maintaining diplomatic relations with the ROC from thirty to twenty-six.[26] Taiwan only gained admission to a small list of international governmental institutions due to pressure from the United States, and by changing its name to avoid offending Beijing.[27] China's diplomatic isolation of the ROC did not yield a thaw in Taiwanese resistance to unification under mainland sovereignty.

While generally employing a tougher approach during the period of Lee's third term, China made conciliatory outreaches to Taiwan's business community.[28] "During the 1995-1996 crisis," Tanner states, "Chinese officials explicitly reassured Taiwan investors that their holdings would be safe."[29] Beijing

[23] Tanner, 48.
[24] Lin, 73.
[25] Bush, 75.
[26] Lin, 65-66.
[27] Bush, 75.
[28] Lin, 66.
[29] Tanner, 113.

also refrained from employing economic coercion against Taiwanese investors after Lee's provocative 1999 statement that "China-Taiwan relations were a 'special form of state-to-state relationship.'" These extensions of olive branches to the Taishang were part of the PRC's inconsistent approach towards recruitment of this group as "conduits of influence."[30]

Tanner contends that Beijing made critical false assumptions about the Taishang's ability to be leveraged by Beijing for its political agenda, asserting: "Beijing's inconsistent tactics, from seductive entreaties to petulant attacks to hollow threats have undermined its own efforts to leverage the Taishang."[31] Surveys of Taiwan business executives revealed that, regardless of their personal political leanings, they did not endorse being used by Beijing as conduits for cross-Strait relations. They preferred to maintain the status quo politically and avoid accusations from the public of selling out Taiwan.[32] [33]

As Lin notes, Beijing's strategies for promoting Taiwanese endorsement of unification backfired, not only failing to sway public opinion on the One China model, but solidifying Taiwanese identity:

> *But Beijing's counterproductive strategy-its demonstrations of military power to influence Taiwanese elections and public opinion-produced a distinct anti-Chinese feeling among most Taiwanese leading to unusual solidarity in support of the government's policy of restricting Taiwanese investment in China. Equally important the missile tests contributed, as polls showed, to the emergence of a Taiwanese identity that would have even longer consequences.*[34]

Surveys reveal a rise from almost twenty percent identifying as Taiwanese in 1996 to over forty percent in 2001. Those claiming dual identity dipped from almost half the population in 1996 to about forty-three percent in 2001. Significantly,

---

[30] Ibid, 111.
[31] Ibid, 112.
[32] Ibid.
[33] Bush, 150-151.
[34] Lin, 87-88.

identification as purely Chinese dropped from over a quarter of the population in 1994 (the highest point in the 1992-1996 surveys) to about ten percent in 2001.[35]

Between 1994-1996, over forty percent of Taiwanese preferred the status quo, with only about twenty percent favoring unification.[36] By 2001, the status quo category had risen to over half the population, while pro-unification dropped slightly.[37] Support for independence, which was about ten percent in the earlier survey, rose slightly to between fifteen to twenty percent in the 1997-2001 data. The statistics for unification changed dramatically if China would become "democratic and prosperous," with nearly half in favor.[38]

These findings show that Beijing's tactics of intimidation failed to sway Taiwanese opinion towards reunification on mainland terms. Even outreach to business leaders was not enough to overcome the deep distrust engendered by the more negative approaches. By the end of Lee's third term, over eighty percent of the population identified as either Taiwanese or dual, with only a minority claiming to be purely Chinese. Only a small percentage favored independence, whereas a strong majority preferred the status quo. Beijing staved off de jure independence, but since Taiwan has political autonomy with its own democratically elected government, maintaining the status quo essentially means de facto independence.

Case Study II: Economic Liberalization: 2008 Election of President Ma Ying-jeou

By the end of Lee's term, the economic costs of restriction of trade with the mainland would become more apparent. In the next election, the DPP candidate, who campaigned on a platform of improving Taiwan's economy by moderating Lee's constraints, prevailed. However, soon after taking office, he started to place economic controls on investment in China, and by his second term, was advocating even stronger restrictions.

[35] Ibid, 55, Figure 3.1 and 92, Figure 4.1.
[36] Ibid, 56 Figure 3.2.
[37] Ibid, 93 Figure 4.2.
[38] Ibid, 56 and 92-93.

His inability to halt the "economic downslide" set the stage for the next episode.[39] In 2008, KMT Ma Ying-jeou was elected with a resounding fifty-eight percent of the vote, with economic issues as the primary motivator.[40] [41] This case study will illuminate the Taiwanese response to the liberalization of cross-Strait economic and cultural ties and a less antagonistic approach from the mainland.

Ma promised improved cross-Strait relations, while simultaneously speaking to the growing sense of Taiwanese identity in calling for "Taiwan's renaissance."[42] Ma campaigned on a platform of increased "prosperity, security, freedom and international dignity by reassuring and cooperating with Beijing." Yet, in his inaugural address, he referred to the Republic of China (ROC) and Taiwan as if they were a single identity, and refrained from using the term PRC when discussing the mainland.[43] With Beijing sensitive to symbolism, these semantic distinctions held significance.

On the issue of reunification, Ma reassured both Washington and Beijing that he would not promote de jure independence.[44] Taiwan experts Bush and Rigger assert that "the true significance of Ma's election" was to clarify that:

> *Taiwan voters would not support a candidate who openly advocated independence and that they preferred a leader who would credibly seek constructive cross-Strait relations (particularly in the economic realm) … and simultaneously resist any outcome with Beijing that did not enjoy broad public support.*[45]

Herein lies the existential Taiwan dilemma of how to capture economic benefits from engagement with China while preserving Taiwan's autonomy by maintaining the status quo. This underlying dichotomy was evidenced in Ma's policy statements designed to pacify Beijing while appeasing his

[39] Ibid, 91, 160.
[40] Ibid, 162.
[41] Bush, 21.
[42] Lin, 162-163.
[43] Bush, 21.
[44] Ibid.
[45] Bush and Rigger, 16.

domestic audience. Maintenance of the status quo and avoidance of unification, as well as military force, were geared to the Taiwanese, whereas the rejection of de jure independence would allay China's fears.[46] Like Lee, Ma stressed the value of democracy and endorsed the "Taiwan first" principle.[47] Although his stated goal was to improve trust and cooperation with Beijing, Tanner states that Ma clearly affirmed the position that unification was contingent on the mainland's democratization.[48] Bush quotes Ma's "intriguing remark that 'in resolving cross-Strait issues, what matters is not sovereignty but core values and way of life.'"[49] Beijing could focus on Taiwan's apparent willingness to abandon the sovereignty issue, whereas the linkage to "core values" would appeal to Taiwanese.

While Ma openly called for negotiations based on the 1992 consensus, his definition of "One China, different interpretations" did not actually align with Beijing's. Bush contends, "In effect, Ma made a bet that China would accept his 1992 consensus pledge as long as the two sides did not dwell on what consensus meant." According to Bush, Ma "sought to foster the PRC's confidence that someday it will achieve its fundamental objectives."[50] Throughout Ma's first term, Beijing and Taipei made progress economically but avoided open political conflict by skirting around any explicit discussion of the underlying dispute.[51]

Under the leadership of Hu Jianto, Beijing took a more conciliatory approach toward Taiwan. Hu announced in 2005 that the foundations for unification would be "safeguarding peace" and "developing cross-Strait relations."[52] In 2008, Hu endorsed taking a gradual approach towards "peaceful development" of cross-Strait relations and advised approaching

[46] Bush, 21-22.
[47] Ibid, 22.
[48] Tanner, 141.
[49] Ibid.
[50] Ibid, 40.
[51] Bush, 41.
[52] Ibid, 36.

skeptical Taiwanese "*with the greatest tolerance and patience*."[53] In response to Ma's liberalization, Hu Jintao issued six proposals for improved cross-Strait relations, including economic cooperation and increased participation by Taiwan in international organizations, contingent on abiding by the "one China" principle.[54] China turned down requests from Paraguay and El Salvador to switch diplomatic recognition to Beijing.[55] However, progress in cross-Strait relations occurred mainly in the economic arena, with little accomplished politically.[56]

With public opinion in 2008 focused on Taiwan's economic interests, "the question," according to Lin, "was not whether Taiwan should expand relations with China, but how far and on what terms."[57] During Ma's first two years as president, Taiwan's growth rate declined significantly.[58] Ma believed that liberalizing cross-Strait relations would revitalize Taiwan's economy after the global economic downturn. He contended that lifting restrictions would yield the additional benefit of convincing China to permit increased Taiwanese participation in regional agreements and in the global economy.[59]

Over the course of Ma's two terms in office, he signed over twenty economic agreements with the mainland,[60] with fourteen concluded in his first two years.[61] Improved economic relations with China boosted trade by 2010, and in this more positive economic environment,[62] the Economic Cooperation Framework Agreement (ECFA) was signed to lift trade barriers further.[63] One benefit of the ECFA was a bilateral dispute-settlement mechanism, which was important due to Beijing's unwillingness to utilize the WTO route because of the

[53] Ibid.
[54] Lin, 172-173.
[55] Ibid, 173.
[56] Bush, 69.
[57] Lin, 205.
[58] Ibid, 168.
[59] Ibid, 163.
[60] Eleanor Albert, "China-Taiwan Relations," June 15, 2018, Council of Foreign Relations, https://www.cfr.org/backgrounder/china-taiwan-relations.
[61] Lin, 163.
[62] Ibid, 168.
[63] Albert.

sovereignty implications.[64] The agreement also conferred trade concessions, investment-protection for the Taishang, and highly favorable terms for investors.[65]

Despite the high level of praise and publicity for the projected impact of these cross-Strait agreements, the actual results were tepid, and there was domestic opposition.[66] [67] While large corporations saw benefits, average citizens failed to reap rewards.[68] The only area to produce significant economic gains was tourism.[69] Even for corporations, implementation was not entirely smooth; difficulties included respect for intellectual property.[70] Furthermore, Taiwan was at a competitive disadvantage in East Asia due to a 2011 free trade agreement (FTA) between China and ASEAN.[71] [72]

Politically, Taiwanese reaction was mixed, with sixty percent of corporate executives favoring economic integration but others, especially the DPP, worried that liberalization could increase dependence and lead to Taiwan becoming a de facto colony to the mainland.[73] The pubic supported trade talks but believed more regulation was necessary and did not endorse cross-Strait liberalization. Ma's low poll ratings stemmed from his inability to revitalize the economy, and his perceived weakness towards Beijing.[74]

Albert highlights public dissatisfaction and mistrust: "Many residents also believe that Ma brought Taipei closer to Beijing without transparency and against the will of the Taiwanese people."[75] Statements from Mainland representatives at a 2009 conference in Taiwan sparked outrage from the DPP, who declared that "the Chinese officials…are in Taiwan to dictate

[64] Lin, 175.
[65] Ibid, 175-176.
[66] Ibid, 163.
[67] Bush, 54.
[68] Albert.
[69] Bush, 54.
[70] Ibid, 51.
[71] Ibid, 50.
[72] Lin, 176.
[73] Bush, 52-53.
[74] Lin, 181.
[75] Albert.

and to threaten – not to listen or learn.."[76] The issue that provoked Taiwanese ire was at the heart of the dilemma: focus on the one-China principle.[77]

These sentiments align with the statistics on preferences for national status. In 2010, only ten percent favored unification, with over twenty percent for independence and sixty percent for the status quo.[78] Economic liberalization and a thaw in negative messaging from Beijing also did not alter the trend on Taiwan's national identity. Over half identified as exclusively Taiwanese, forty percent as dual, and less than five percent as Chinese.[79] A 2017 survey showed that national identity had stabilized, with fifty-five percent identifying as Taiwanese alone, thirty-seven percent as dual, and only Chinese remaining at about four percent.[80]

Albert attributes this trend to the maturation of Taiwan's democracy: "Generations of democratic practices seem to have bound together the Taiwanese people and polity."[81] By the end of Ma's presidency, disapproval for his "China warming policies" led to KMT electoral losses.[82] China was no closer to reunification.

Conclusion

An examination of these two case studies reveals that, regardless of the party in power in Taiwan, and whether or not China used the carrot or the stick approach, the Taiwanese people have been moving further away from reunification under PRC rule. Instead of bringing Taiwan into a closer relationship with the mainland, Hu Jintao's more positive overtures in response to Ma's economic liberalization failed to meet with widespread public approval in Taiwan. As Bush notes, economic integration does not automatically translate

[76] Bush, 70-71.
[77] Ibid, 70.
[78] Lin, 166, Figure 6.2.
[79] Lin, 165, Figure 6.1.
[80] Albert.
[81] Ibid.
[82] Ibid.

into political integration.[83] While Beijing's strategy of military intimidation during Lee's presidency may have strengthened Taiwanese fear of declaring outright de jure independence, it did not yield support for reunification.

China had believed that the missile tests in 1995-1996 would push the electorate into embracing a KMT government more favorable to Beijing. Paradoxically, the military exercises further alienated the Taiwanese people and provoked economic restrictions by President Lee. Significantly, China's abrasive actions correlated with a consolidation of Taiwan's sense of national identity, and this trend continued, even under Ma's "China warming policies." The underlying issue seems to have been a deep mistrust of Beijing engendered by the contradictory policies and history of intimidation, in combination with the failure of economic liberalization to revive Taiwan's domestic economy.

Taiwan has been torn between motivation to improve its economy, through increased trade with China, and fear of dependency. As political economist Lin notes, "Taiwan faces a rare dilemma in that its most important economic partner is also an existential threat."[84] The growing power asymmetry has only exacerbated this problem. Under the current president, Xi Jinping, China is unlikely to democratize anytime soon. In response to the 2016 election of DPP candidate Tsai and her refusal to accept the 1992 consensus, Xi issued a warning against independence and reconfirmed China's willingness to use force if that were to occur.[85] [86]

Beijing's continued efforts to influence the media and elections in Taiwan, as well as their intrusive interjections in Hong Kong

---

[83] Bush, 66

[84] Lin, 1.

[85] Abraham Denmark, "China's Increasing Pressure on Taiwan," January 30, 2018, Wilson Center, https://www.wilsoncenter.org/blog-post/chinas-increasing-pressureTaiwan.

[86] Bonnie S. Glaser, "Managing Cross-Strait Ties in 2017: Recommendations for the Trump Administration," January 2017, Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170202_Glaser_ManagingCrossStraitTies2017_Web_2.pdf, accessed October 15, 2020.

governance, have thus far failed to sway Taiwanese opinion away from support for their own democracy. The trend towards increased Taiwanese identity, which corresponds to the establishment of Taiwan's democracy, continues to this day.[87] Recent events in Hong Kong have only served to dramatically strengthen Taiwan's resolve to preserve their rights. The protest movement and the steps to curtail freedom in Hong Kong that motivated the dramatic response of its citizens clearly revealed the lack of validity of the "one country-two systems model." Beijing's erosion of free and fair elections by allowing only PRC-approved candidates and the attempt to change the venue for trying Hong Kongers accused of a crime to mainland China demonstrate that the acclaimed "two systems" model of governance is merely phase I in a plan towards full integration of all Chinese territory into the CCP's tight control.

Taiwan's response to events in Hong Kong was the overwhelming reelection of President Tsai, despite strong efforts from Beijing to interfere on behalf of her KMT opponent. "Democratic Taiwan and our democratically elected government will not concede to threats and intimidation," Tsai declared to throngs of enthusiastic supporters after her landslide victory. Just six months earlier, Tsai's prospects did not appear bright. The Kuomintang candidate, Han Kuo-yu, touted forthcoming economic benefits and security resulting from closer ties with Beijing. Polls showed him ahead.[88]

At a rally on the eve of the election, Tsai clearly tied the fate of Hong Kong to Taiwan's critical choice in the path forward: "Young people in Hong Kong have used their lives and shed their blood and tears to show us that 'one country, two systems' is not feasible. Tomorrow, it is the turn of young people of Taiwan to show Hong Kong that the values of

[87] David An, et al. "Swinging the Vote: How the CCP influences the Media and Elections in Taiwan and Beyond" (speech, Global Taiwan Institute, Washington DC, June 13, 2019).

[88] Emily Feng, "Rebuking China, Taiwan Votes To Reelect President Tsai Ing-wen," January 11, 2020, *NPR*, https://www.npr.org/2020/01/11/795573457/rebuking-chinataiwan-votes-to-reelect-president-tsai-ing-wen.

democracy and freedom overcomes [sic] all difficulties."[89] Fear of losing their democratic way of life propelled voters to support the anti-reunification candidate. The Taiwanese value of freedom underlies the contradictory approach to economic integration and strong opposition to political reunification with China.

[89] Ibid.

A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy

Wade H. Atkinson, Jr.

The Trump Administration's National Cyber Strategy (NCS) was published in 2018 in a rapidly evolving threat environment due to the verification of increasingly sophisticated threats in cyber espionage, cyber physical attacks, and electoral manipulations. The NCS attempts to use a "whole of government" approach to Protect the Homeland, Promote American Prosperity, Preserve Peace Through Strength, and Advance American Influence (the "Four Pillars" of U.S. Cyber Strategy). At its core, the National Cyber Strategy seeks to use a renewal of the historic American Public-Private Partnership, which evolved from the post-World War II Defense Industrial Base to all forms of U.S. cyber security via real-time, comprehensive, and well-protected information-sharing among all critical U.S. entities about threat/defense/response actions.

From the Cold War to the Cyber Era

The post-Cold War era has seen a dramatic increase in cyber espionage, cyber attacks on physical entities, and cyber manipulation of democratic processes and elections. Those attacks have, in turn, required the progressive focus of U.S. administrations, beginning with Presidents Ronald Reagan, George H.W. Bush, Bill Clinton, George W. Bush, and

Barrack Obama. In the words of one author, "in the eight years [Obama was] in the White House…cyber went from a nuisance to a mortal threat."[1] This led to the Trump Administration's Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 20, 2017) and culminated in the Trump Administration's "National Cyber Strategy of the United States of America," issued in September 2018.

The new "Cyber Era"[2] of fast-paced cyber offense and defense has seen various forms of intrusions, attacks, and manipulations, which can be broken down into three categories: cyber espionage intrusions (often with economic and geopolitical consequences), cyber attacks which resulted in physical and economic damage, and cyber manipulations of democratic processes and elections.

The first category of cyber espionage intrusions would include espionage-oriented cyber network intrusions with nicknames such as "Titan Rain," "Mafia Boy," "Epsilon," "Morris Worm," and the Chinese breach of the U.S. Office of Personnel Management ("OPM"). The second category of cyber attacks – attacks which resulted in physical and economic damage – include the original U.S. "logic bomb" which blew up the Soviet Siberian gas pipeline in 1982; the U.S./Israeli Stuxnet virus, which severely damaged Iranian nuclear centrifuges in 2010; the Iranian attack on Saudi ARAMCO in 2012, which resulted in severe economic and network damage to ARAMCO; the Iranian attack on the Bowman Avenue Dam in Rye, New York in 2013; the North Korean attack on Sony Pictures in 2014; and the Russian attack on the Ukrainian power grid in 2015. The third category of cyber manipulations of democratic processes and elections includes the Russian and

[1] Quoting David E. Sanger, *The Perfect Weapon*, (New York, New York: Penguin, 2018), p. 146.

[2] The "Cyber Era" refers to a new era in international relations which offers new opportunities for political cooperation, but also disrupts interstate dealings and empowers subversive actors. See, Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), Chapter 3 on "Technical Revolutions and International Order, pp. 80-115.

Chinese use of social media platforms, such as Facebook, Google, and Twitter, to polarize electorates/disrupt democratic processes/manipulate elections in the U.S., U.K., and Germany from at least 2016 to the present.

Development of U.S. National Cybersecurity Policy from Presidents Reagan to Obama

Beginning with the Reagan Administration's National Security Decision Directive Number 145 (NSDD-145) on September 17, 1984, the U.S. national security apparatus set up systems and processes (including a National Manager for Telecommunications Security and Automated Information Systems Security) to examine government telecommunications systems and automated information systems, to evaluate U.S. vulnerability to hostile interceptions and exploitation, and to use the National Bureau of Standards for Federal Information Processing Standards.[3] The George H.W. Bush Administration in National Security Directive-42 (NSD-42) of July 5, 1990, established a National Security Council/Policy Coordination Committee for National Security Telecommunications and Information Systems to provide systems security guidance for national security systems.[4] The Clinton Administration, in Presidential Decision Directive (PDD-63) of May 22, 1998, explicitly recognized the mutually reinforcing and dependent nature of the U.S. public and private sectors with the U.S. as the world's strongest military and its largest national economy.[5] The Clinton Administration recognized the interdependence of the U.S. economy and military on "certain critical infrastructure and cyber-based information systems for

[3] National Security Policy Directive Number 145 (Washington, D.C.: The White House, September 17, 1984). https://fas.org/irp/offdocs/nsdd145.htm, accessed October 7, 2020.
[4] National Security Directive Number 42 (Washington, D.C.: The White House, July 5, 1990). https://fas.org/irp/offdocs/nsd/nsd42.pdf, accessed October 7, 2020.
[5] Presidential Decision Directive Number 63 (Washington, D.C.: The White House, May 22, 1998) https://fas.org/irp/offdocs/pdd/pdd-63.htm, accessed October 7, 2020. See also, William J. Clinton, "A National Security Strategy for a New Century" (Washington, D.C. The White House, October 1988), p. 17. https://clintonwhitehouse4.archives.gov/media/pdf/nssr-1299.pdf, accessed October 7, 2020.

the minimum operations of the economy and government in defense, telecommunications, energy, banking and finance, transportation, water systems, and emergency services."[6] The Clinton Administration set the year 2003 as the deadline for achieving and maintaining the ability to protect the nation's critical infrastructure from intentional attacks. NPP-63 also recognized that the elimination of potential U.S. vulnerability required "a closely coordinated public-private partnership to reduce vulnerability."[7] NPP-63 designated for each sector of the economy vulnerable to an infrastructure attack a designated Lead Agency Senior Sector Liaison to work with the private sector and to develop a sectoral National Infrastructure Assurance Plan.

Perhaps most significantly for the development of the U.S. Cybersecurity Public-Private Partnership ("PPP"), the Clinton Administration's NPP-63 initiated the use of Information Sharing and Analysis Centers ("ISACs").[8] In ISACs, critical infrastructure owners and operators are brought together "to collect, analyze, and disseminate actionable threat information and provide members tools to mitigate risks and enhance resiliency."[9] The Clinton Administration initiated the establishment of an ISAC, originally for each of the then seven designated critical infrastructure sectors, to coordinate with

---

[6] Presidential Decision Directive Number 63. https://fas.org/irp/offdocs/pdd/pdd-63.htm, Accessed October 7, 2020. See also, Meagan Brown, "Cyber Imperative: Preserve and Strengthen Public-Private Partnerships" (White Paper) (Arlington, VA: George Mason Antonin Scalia School of Law, National Security Institute, 2018), pp. 1-2. https://nationalsecurity.gmu.edu/cyber-imperative-preserve-and-strengthen-public-private-partnerships/, accessed October 7, 2020.

[7] National Security Directive Number 63, p. 3. Indeed, the George W. Bush Administration National Security Council worked diligently during 2001-2009 to protect critical aspects of the national infrastructure. See generally, Michael Chertoff, *Exploding Data: Reclaiming Our Cybersecurity in the Digital Age* (New York, New York: Atlantic Monthly Press, 2018).

[8] See Megan Brown, "Cyber Imperative: Preserve and Strengthen Public-Private Partnerships" (White Paper) (Arlington, VA: George Mason Antonin Scalia School of Law, National Security Institute, 2018.) https://nationalsecurity.gmu.edu/cyber-imperative-preserve-and-strengthen-public-private-partnerships/, accessed October 7, 2020.

[9] National Council of Information Sharing Analysis Centers (ISAC's), "About ISACs." https://www.nationalisacs.org/about-isacs, accessed October 7, 2020.

each other across sectors and with the government.[10] For instance, the first, the Financial Services ISAC ("FS-ISAC") was formed in 1999 and has been operating for nearly 20 years. The Communication ISAC, also known as the DHS National Coordinating Center, is part of DHS's National Cybersecurity and Communications Integration Center ("NCCIC") – "the national nexus of cyber and communications integration for the Federal Government, the Intelligence Community, and Law Enforcement."[11] More ISACs were formed and expanded during the Clinton and Bush Administrations and constitute one of the central hubs of the U.S. public-private partnership in cybersecurity. To date, ISACs have been established in 18 areas: Automotive, Aviation, Communication, Defense-Industrial Base, Downstream Natural Gas, Electricity, Emergency Management and Response, Financial Services, Health Information Technology, Multi-State (state, local, tribunal, and territorial governments), National Defense, Oil and Natural Gas, Real Estate, Research and Education Networks, Retail Businesses, Surface and Public Transportation, and Water and Wastewater.[12] Most recently, the Automotive ISAC ("Auto-ISAC") signed a Cooperative Research and Development Agreement ("CRADA"), with DHS allowing for public-private collaboration with DHS on cyber threats to automated vehicles in order to detect and prevent vehicular cybersecurity threats. The CRADA allows Auto-ISAC members to obtain security clearances, access government facilities, and collaborate with DHS on issues relating to potential cybersecurity threats to automated vehicles."[13]

Following 9/11 and the creation of the Department of Homeland Security ("DHS") in 2001, the George W. Bush Administration formally addressed the issue of cybersecurity as part of the renewed interest in U.S. homeland security and

[10] National Council of Information Sharing Analysis Centers (ISAC's), "About ISACs." https://www.nationalisacs.org/about-isacs, accessed October 7, 2020.
[11] Quoting Brown, "Cyber Imperative," p.4.
[12] National Council of Information Sharing Analysis Centers (ISAC's), "About ISACs." https://www.nationalisacs.org/about-isacs, accessed October 7, 2020.
[13] Brown, "Cyber Imperative," p.5.

simultaneously issued National Security Presidential Directive (NSPD-54) and Homeland Security Presidential Directive (HSPD-23) on January 8, 2008.[14] These documents' goal was to provide an "enduring and comprehensive approach to cybersecurity that anticipates future cyber threats and technologies and involves applying all elements of national power and influence to secure national interests in cyberspace."[15] NSPD-54/HSPD 23 also established the National Cyber Response Coordination Group ("NCRCG") and the National Cybersecurity Center ("NCC") at DHS. HSPD-23 tasked the Secretary of Homeland Security to prepare a report detailing policy and resource requirements for improving the protection of privately-owned U.S. critical infrastructure networks. In the post-9/11 environment, DHS increasingly became the centerpiece of U.S. non-defense and intelligence cybersecurity under its second Secretary, former U.S. Appellate Court Judge Michael Chertoff, who served from 2005-2009.[16]

The Obama Administration placed increased emphasis on cybersecurity and signed Executive Orders and National Security Presidential Directives (many of which are still classified) to bolster America's response to cyber intrusions and cyber attacks. The Obama Administration also championed PPPs and the use and expansion of ISACs. Executive Order 13691 on "Promoting Private Sector Cybersecurity Information-Sharing" called on DHS "'to develop a more efficient means for granting clearances to private sector individuals' in Information Sharing and Analysis Organizations ('ISAOs') and to "identify a set of voluntary standards or guidelines" for them," especially for sectors that, due to their unique needs, "cannot join an ISAC, but still have a need for

[14] National Security Presidential Directive Number 54; Homeland Security Presidential Directive Number 23 (Washington, D.C.: The White House, January 8, 2008). https://fas.org/irp/offdocs/nspd/nspd-54.pdf, accessed October 7, 2020.
[15] National Security Presidential Directive Number 54. p. 1 emphasized the need for public-private information sharing in cybersecurity to be coordinated primarily by DHS, with the exception of the defense, defense-industrial, and intelligence sectors, which were to be coordinated by DOD.
[16] See, Michael Chertoff, *Exploding Data: Reclaiming Our Cybersecurity in the Digital Age* (New York, New York: Atlantic Monthly Press, 2018), pgs. 1-25.

cyber threat information and can benefit from membership in an ISAO."[17] Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity" emphasized the centrality of the PPP to the Obama Administration's cybersecurity strategy. EO 13636 stated that: "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and… [promote innovation and efficiency] …through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[18]

The Trump Administration National Cyber Strategy

The Trump Administration's "National Cyber Strategy" was articulated in a rapidly evolving threat environment due to the verification of increasingly sophisticated threats in cyber espionage, cyber physical attacks, and electoral manipulations by criminal groups, state and non-state actors, and combinations of state and non-state actors. The public nature of the Sony Pictures attack, combining a devastating physical and economic attack on a U.S. commercial entity with related credible threats of domestic terrorism, and the lack of a clear response by the Obama Administration, crystallized the need for a National Cyber Strategy.[19]

The Trump National Cyber Strategy had its origins in Presidential Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 20, 2017), which dealt primarily with federal networks, procurement, and information infrastructure.[20] The lead agencies named in Executive Order 13800 were DHS and

---

[17] Brown, Cyber Imperative, pp. 4-5.
[18] Executive Order 13636 (Washington, D.C.: The White House, February 12, 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, accessed October 7, 2020.
[19] See, Sanger, *The Perfect Weapon*, pgs. 124-151.
[20] Executive Order 13800 (Washington, D.C.: The White House, May 20, 2107), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/, accessed October 7, 2020.

OMB (for all aspects of cybersecurity other than defense and intelligence) and DOD and DNI (for defense and intelligence network and infrastructure).[21]

Section 2 (a) of Executive Order 13800 stated:

> *It is the policy of the Executive Branch to use its authorities and capabilities to support the cybersecurity and risk management efforts of the owners and operators of the Nation's Critical Infrastructure (as defined in Section 5195 (c) (e) of Title 42, USC) (critical infrastructure entities), as appropriate.*[22]

Title 42, U.S.C. Section 5195 (c) (e), as adopted by the Patriot Act of 2001, defines critical infrastructure as:

> *…The term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[23]

Executive Order 13800, Section 4 (a) also defines "appropriate stakeholders" as "any non-executive branch, person, or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and Secretary of Homeland Security under Section 2 (d) of EO 13800."[24]

---

[21] Executive Order 13800, p.5. The Department of Defense (DOD) was named as the Sector-Specific Agency for the Defense, Defense Industrial Base (DIB), and Intelligence Sectors. DOD is "responsible for leading the collaborative coordinated effort to identify, assess, and improve the risk management of critical infrastructure across the DIB with its partners." See, Department of Homeland Security and Department of Defense, "Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Plan" (NIPP) (2010), Preface, p. iii. https://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf, accessed October 7, 2020.

[22] Executive Order 13800, p.5, quoting 42 U.S.C. Sec. 5195 9 (c) (e)'s definition of "critical infrastructure."

[23] Quoting Title 42, United States Code, Section 5195c (e) (2018). https://www.law.cornell.edu/uscode/text/42/5195c, accessed October 7, 2020.

[24] Quoting Executive Order 13800, p. 10.

(Section 2 (d) of EO 13800 refers specifically to Resilience Against Botnets and Other Automated Distributed Threats).[25]

Following on Executive Order 13800, in September 2018, the Trump Administration issued its "National Cyber Strategy of the United States of America." This document put forth the "Four Pillars" of U.S. Cyber Strategy: Protecting the American People, the Homeland, and the American Way of Life (Pillar I); Promoting American Prosperity (Pillar II); Preserving Peace Through Strength (Pillar III); and Advancing American Influence (Pillar IV).[26]

In its Cover Letter and Introduction, the Trump Administration National Cyber Strategy issued a "call to action for all Americans and our great companies to take the necessary steps to enhance our national security"[27] in order "to reflect our principles, protect our security, and promote our prosperity based on the American values of individual liberty, free expression, free markets, and privacy.[28]

Pillar I on "Protecting the American People, the American Homeland, and the American Way of Life" focuses on Securing Federal Networks and Information, Securing Critical Infrastructure (as previously defined in 42 USC Sec. 5195 (c)(e)), and Combatting Cybercrime and Improving Incident Reporting.[29] Pillar I discusses protecting information networks, whether public or private, by both the public and private

---

[25] Executive Order 13800, p. 5. "Botnets" are a network of private computers infected with malicious software and controlled as a group that can operate without the owner's knowledge. They can be used to perform distributed denial-of-service (DDOS) attacks, steal data, send spam, and allow the attacker to access devices and connections.

[26] "National Cyber Strategy of the United States of America" (Washington, D.C.: The White House, September 2018). https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed October 7, 2020.

[27] Quoting President Trump's Transmittal Letter of National Cyber Strategy, p. ii. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed October 7, 2020.

[28] National Cyber Strategy (NCS), pp i-ii advances the use of the NCS to promote national security and also benefit the U.S. economically. See, NCS, Pillar II on "Promoting American Prosperity," pp. 8-14.

[29] The National Cyber Strategy picks up the definition of "Critical Infrastructure" from EO 13800.

sectors as a "responsibility shared by the private sector and the federal government."[30] This is to be done, in part, by managing supply chain risk in the nation's infrastructure, using federal cyber standards (particularly in the defense-industrial base), and by adopting a risk management approach to mitigate vulnerabilities and raise the base level of cybersecurity across the critical infrastructure areas of national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation.[31] Implementation of industry-driven certification regimes, incentivization of cybersecurity investments (presumably through the U.S. Tax Code), and creation of a National Critical Infrastructure Security Resilience Research and Development Plan to protect key infrastructure assets (such as assets for positioning, navigating, and timing (PNT assets), which are crucial to so many U.S. defense and consumer electronic devices) are the preferred means for achieving these objectives.[32] Pillar I also discusses the use of U.S. law enforcement to work with private industry to disable cybercriminal infrastructure (botnets and dark markets) and to confront challenges presented by technological barriers (such as anonymization and encryption technologies) to obtain time-sensitive evidence for appropriate legal processes.[33] In order to do this, the Trump Administration proposes to work with Congress to update electronic surveillance and computer crime statutes, use law enforcement tools to investigate and prosecute transnational crimes in cyberspace, and promote international law enforcement cooperation by use of the U.N. Convention on Transnational Organized Crime, The G-7 24/7

[30] National Cyber Strategy, pp. 8-11. The lead agencies for protecting critical information networks are DHS and DoD (for defense, defense industrial base, and intelligence.).

[31] National Cyber Strategy, pp. 8 - 11. Ultimately 18 areas of critical infrastructure have been designated. Each industry sector will use designated experts to facilitate the exchange of information. For instance, for Defense, the Defense Industrial Base (DIB), and Intelligence, DoD has been designated.

[32] National Cyber Strategy, pp. 8-11.

[33] National Cyber Strategy, pp. 8 -11. This will be composed of law enforcement partners at the federal, state, local, and tribal levels.

Network Points of Contact Program, and the expansion of the Council of Europe's Budapest Convention on Cybercrime.[34]

Specifically, Section 3 of Pillar I, on "Securing Critical Infrastructure," discusses the need to "Leverage Information and Communication Technology Providers as Cybersecurity Enablers." It states:

> *Information and communications technology (ICT) underlies every sector in America. ICT providers are in a unique position to detect, prevent, and mitigate risk before it impacts their customers, and the Federal Government must work with these providers to provide ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties. The United States Government will strengthen efforts to share information with ICT providers to enable them to respond and remediate known malicious cyber activity at the network level. This will include sharing classified threat and vulnerability information with cleared ICT operators and downgrading information to the unclassified level as much as possible. The U.S. will promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards. The United States Government will convene stakeholders to devise cross-sector solutions to challenges at the network, device, and gateway layers, and we will encourage industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape.*[35]

In Pillar II on "Promoting Prosperity," the Trump Administration says that it expects the technology marketplace to support and reward the continuous development, adoption, and evolution of innovative scientific technology and processes by promoting best practices and developing strategies to

---

[34] Id., p.11. While the Trump Administration has encouraged international law enforcement cooperation by use of the UN Convention on Transnational Organized Crime, the G-7 24/7 Network Points of Contact Program, and the expansion of the Council of Europe's Budapest Convention on Cybercrime, it has not endorsed a Comprehensive International Cybersecurity Treaty/Code of Conduct. See, https://www.state.gov/release-of-the-2018-national-cyber-strategy.

[35] Quoting, National Cyber Strategy, pp. 8-9.

overcome market barriers to adoption of secure technologies.[36] The Administration will improve awareness and transparency of cybersecurity practices to build market demand for more products and services in collaboration with international partners. This will be done by encouraging "best practices" in industry and facilitating next-generation telecommunications and information infrastructure in the U.S. using the evolution of 5-G technology, spectrum-based solutions, and emerging technologies, such as artificial intelligence (AI), quantum computing, and next-generation telecommunications infrastructure.[37] The Administration also proposes the free flow of data, digital trade, and cybersecurity innovation through "trade-related engagement, innovative tools, and best uses, in order to achieve full life-cycle cybersecurity using things such as strong default settings, upgradeable products, and best practices to differentiate products based on security features and foundational engineering practices."[38] In order to achieve this, the U.S. will use strong intellectual property rights enforcement, the CFIUS process, and administrative enforcement agencies, such as the FCC, the FTC, and (presumably) the newly-created Cybersecurity and Infrastructure Security Agency to be created from the former DHS National Protection and Programs Directorate ("NPPD").[39] Additionally, the Trump Administration proposes the development of a stronger U.S. cybersecurity workforce, through education, training, and the National Institute for Cybersecurity Education, which will educate and re-train

---

[37] National Cyber Strategy, p.14.

[37] National Cyber Strategy, p. 14-15. Pillar II proposes a more nationalistic approach to cybersecurity. For instance, the Trump Administration has opposed the sale of 5-G equipment in the U.S. by China's Huawei on national security grounds. See, https://www.cnn.com/2019/07/04/tech/huawei-us-ban.

[38] National Cyber Strategy, pp. 14-17. This goal echoes the December 2017 National Security Strategy of the U.S. generally, and specifically with regard to cybersecurity. See, National Security Strategy of the U.S. at pp. 12-14 on "Keep America Safe in the Cyber Era"; pp.20-21 on "Lead in Research, Technology, and Innovation"; p. 29 on "Defense Industrial Base"; and p. 31-32 on "Cyberspace" and "Intelligence."

[39] See Charlie Mitchell, "Long-Awaited Cyber Agency Nears, But Will It Change Anything Much?" in *The Washington Examiner*, October 23, 2018, discussing the likely passage of the Cyber Act of 2015, currently in House-Senate Conference Committee. https://www.washingtonexaminer.com/policy/technology/long-awaited-cyber-agency-nears-but-will-it-change-anything-much, accessed October 7, 2020.

secondary, post-secondary, vocational, and professional levels.[40]

In Pillar III on "Preserving Peace Through Strength," the Trump Administration says that it will integrate the employment of cyber options across every element of U.S. national power using an integrated diplomatic, military, economic, and law enforcement approach to promote the U.S. national interest and preserve the U.S. "overmatch" in cyber technology.[41] For instance, it will encourage universal adherence to cyber norms, international law, and voluntary non-binding norms to achieve predictability and stability in cyberspace. It will also use the U.S. intelligence community and the U.S. International Cyber Deterrence Initiative to counter malign influence and information campaigns by working with "foreign government partners, the private sector, academia, and civil society."[42]

Finally, in Pillar IV on "Advancing American Influence," the Trump Administration promises a multi-stakeholder model of Internet governance based on a "transparent, bottom-up, consensus-driven process that enables governments, the private sector, civil society, academia, and the technical community to participate on an equal footing," using diverse organizations, such as the Freedom Online Coalition, The Internet Governance Forum, and the U.N. Telecommunications Union, "to promote interoperable and reliable community infrastructure and Internet connectivity."[43] Pillar IV states this can be achieved by "working with like-minded countries,

---

[40] National Cyber Strategy, pp. 14-15.

[41] Id., pp. 20-21. This goal of "overmatch" reinforces what was previously stated in The National Security Strategy of the U.S., pp. 12-14 and pp. 31-32.

[42] Id. This threat/goal is reiterated in the January 29, 2019 Worldwide Threat Assessment of the U.S. Intelligence Community on "Cyber." https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf, accessed October 7, 2020. See, Worldwide Threat Assessment of the U.S. Intelligence Community, (Testimony of Daniel R. Coats, Director of National Intelligence to the Senate Select Committee on Intelligence, January 29, 2019) pp.5-7. https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf, accessed October 7, 2020.

[43] Id., pgs. 24-26. See, also, Madeline Carr, "Public-Private Partnerships in National Cybersecurity Strategies" in *International Affairs* 92:1 (2016).

industry, civil society, and stakeholders through integrated technical development, digital safety, training, policy advocacy, and research.[44] A priority will be enhancing Cyber Capacity Building Efforts "as building blocks for organizing national efforts for cybersecurity, sharing information, and threat warnings, cybersecurity coordination, and promoting analytical and technical exchanges in order to promote markets for American ingenuity overseas, including for emerging technologies, which can, in turn, lower the cost of security."[45]

The Trump Administration has gone out of its to emphasize the PPP in its cybersecurity strategy. For instance, at the 2018 DHS National Cybersecurity Summit, Vice President Pence stated: "Cybersecurity is a shared responsibility and the President and I need you to be advocates in your industry and among your peers for greater cybersecurity collaboration."[46] In addition to EO 13800 on "Strengthening the Cybersecurity of the Federal Networks and Critical Infrastructure" and the "National Cyber Strategy," the recent "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated Distributed Threats," noted the importance of public-private partnerships and called for "collaboration to improve the ability of the ecosystem members to mitigate botnet threats."[47]

---

[44] Id. However, the U.S. Department of State still opposes a Comprehensive International Cybersecurity/Code of Conduct. See https://www.state.gov/release-of-the-2018-national-cyber-strategy/, accessed October 7, 2020.

[45] National Cyber Strategy, p. 26.

[46] Remarks of Vice President of the United States Mike Pence at the DHS Cyber Summit (Washington, D.C.: The White House, July 31, 2018.) https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-dhs-cybersecurity-summit/, accessed October 7, 2020.

[47] U.S. Department of Commerce and Department of Homeland Security, "Enhancing the Resilience of Internet Communications Ecosystem Against Botnets and Other Automated Distributed Threats" (May 22, 2018). https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final, accessed October 7, 2020.

Wade H. Atkinson, Jr.

The Evolution of the Public-Private Partnership in U.S. Cybersecurity Policy

At its heart, the Trump Administration National Cyber Strategy relies on a dramatic evolution in the nature of the Public-Private-Partnership (PPP) in U.S. national security by relying on continuous information-sharing and coordination, rather than manufacturing or production, to protect the U.S. from cyber espionage, cyber attacks, and cyber manipulation.

Historically, the U.S. private sector has always supported the U.S. national security sector enormously, and virtually unconditionally, with the building of ships, tanks, planes, and satellites, as well as large-scale, technology-driven projects, such as the Manhattan and the Apollo Projects; the integration of stealth technology and precision-guided weapons into military arsenals; and the Strategic Defense Initiative (SDI). These programs and projects enriched the private sector with government contracts and the public good with related security and technology innovations. The U.S. PPP grew out of necessity during the American Revolution and the War of 1812, continued through the U.S. Civil War, and was firmly established in the Presidential Emergency Powers granted under the Trading with the Enemy Act of 1918. President Franklin Roosevelt used the Trading with the Enemy Act to expand Presidential powers during the New Deal and for war preparation prior to the U.S. entry into World War II. Certain aspects of the PPP were expanded in the 1952 National Defense Act, which created the National Security Resources Board.[48] Generally, the PPP worked quite well through the Vietnam Era; contributed greatly to the Strategic Defense Initiative, which won the Cold War; and propelled the technology-driven integrated battle strategies, which won the two Gulf Wars in 1994 and 2003, in dramatic fashion.

However, the Trump Administration's adaption of the PPP in its National Cyber Strategy represents a departure, by

[48] See Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies" in *International Affairs* 92:1 (2016). pgs. 46-49

necessity, from the traditional PPP because it involves a continuous sharing and coordination of code, information, data (including trade secrets and proprietary data), and information/communication technology, not manufacturing or production, in a never-ending offensive and defensive cybersecurity effort. This multifaceted and continuous offensive and defensive use of the PPP, domestically and internationally, will present unparalleled challenges in the Cyber Era.

The Cybersecurity Imperative

The cyber threat poses unique threats to U.S. economic and national security because of its inherently global nature; the extremely rapid evolution of technology and tactics; the involvement of criminal, state, and non-state actors; and the dynamics of a partnership/consensus approach "along with some necessary elements of a regulatory approach" to the public-private nature of cyber challenges. An estimated 80% of U.S. critical infrastructure is owned and operated by the private sector, and most U.S. digital services were created by the domestic innovation base.[49] Yet, many aspects of the information and communication technology (ICT) sector are also regulated by government agencies, such as the FCC, the FTC, and the SEC. Therefore, a cooperative, but sometimes enforceable/deferential, public-private "partnership" is required across industries to better defend critical systems and functions from adversaries, while protecting the American public from predatory business practices at home.[50] For instance, the government (the public entity in the PPP) must regulate certain aspects of the private entities it is partnering with to prevent private citizens from dangers, such as corporate pricing or access abuses. At the same time, the government needs cooperation from the private sector,

[49] See, Cybersecurity Information Agency Release on the Defense Industrial Sector, https://www.cisa.gov/defense-industrial-base-sector, accessed October 7, 2020.
[50] See, DHS and DOD Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, p.3, https://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf, accessed October 7, 2020.

particularly the ICT sector, to perfect and preserve infrastructure and security standards. Put another way: "A unity of effort is required by those responsible for protecting the nation and those who own and operate the infrastructure that is critical to the mission."[51]

Public-private partnerships do exist across federal agencies and are often championed by the National Institute of Standards and Technology ("NIST") whose mission is: "to assist private sector initiatives to capitalize on advanced technology; to advance through cooperative efforts among industries, universities, and government laboratories, promising research and development projects, which can be optimized by the private sector for commercial and industrial applications; and to promote shared risks, accelerated development, and pooling of skills which will be necessary to strengthen America's manufacturing industries."[52] NIST's cybersecurity role has evolved under the Cybersecurity Enhancement Act of 2014, which directs NIST to "facilitate and support the development of voluntary consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risk to critical infrastructure.[53] Private collaboration was crucial to NIST's "Framework for Improving Critical Infrastructure Cybersecurity" developed in a year-long collaborative process. NIST serves as a convener for industry, academia, and government stakeholders, while DHS coordinates much of the information-sharing between the government and the private sector using the ISACs.

DHS is also developing other information-sharing technologies. For example, Automated Indicator Sharing ("AIS") managed by DHS U.S. Computer Emergency Readiness Teams (US-CERT)

---

[51] Quoting, Brown, "Cyber Imperative," p. 10.
[52] See, 15 U.S. Code 271 defining the role of the National Institute of Standards and Technology (NIST), https://www.law.cornell.edu/uscode/text/15/271, accessed October 7, 2020.
[53] Cybersecurity Enforcement Act of 2014, Sec. 101, Pub. L. No. 113-274, 128 Stat. 2971 (2014), https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf, accessed October 7, 2020.

aims "to enable the exchange of threat indicators between the Federal Government and the Private Sector at machine speed."[54] The DHS Office of Cybersecurity and Communications leads efforts to protect the federal government networks and to collaborate with the private sector to increase the security of critical networks.[55] DHS also announced the establishment of a National Risk Management Center to be the gateway for American companies to work with the federal government more closely to strengthen our shared cybersecurity.[56] Furthermore, the efforts at DHS to emphasize the collaboration have been increased by raising the profile and mission of the National Protection and Programs Directorate (NPPD) to become an independent agency: The Cybersecurity and Infrastructure Security Agency, pursuant to the Cyber Security Act of 2015.[57] Presumably, the new Cybersecurity and Infrastructure Security Agency will streamline the functions of the old NPPD. However, as envisioned, it still lacks a Division of Enforcement, similar to the Divisions of Enforcement of the SEC, CFTC, or FTC to serve as an investigatory/enforcement/international-information-sharing arm to enforce the 11 cybersecurity statutes Congress passed in 2014 and 2015. Therefore, the Cybersecurity and Infrastructure Security Agency will apparently have to rely on cooperation and information-sharing, rather than administrative enforcement, and refer civil, administrative, and criminal cases to the Department of Justice (DOJ).

Sector-specific Departments and Agencies have embraced the PPPs as well, including the Department of Energy, which has a Multiyear Plan for Energy Sector Cybersecurity; the FCC, which has a Communications Security, Reliability, and Interoperability Council ("CSRIC"); and the FDA, which is

---

[54] United States Computer Emergency Readiness Team ("US-CERT"), "Automated Indicator Sharing," https://www.us-cert.gov/ais, accessed October 7, 2020.
[55] DHS, Office of Cybersecurity Communications, https://www.hsdl.org/?abstract&did=440227, accessed October 7, 2020. https://www.cisa.gov/cybersecurity-division, accessed October 7, 2020.
[56] CISA, National Risk Management, https://www.cisa.gov/national-risk-management, accessed October 7, 2020.
[57] See Mitchell, "Long-Awaited Cyber Agency Nears", pp. 14-15.

developing a Cyber Med (Expert) Analysis Board to complement existing device vulnerability coordination and response mechanisms.[58]

Similarly, Congress has developed a collaborative consensus-driven approach over a regulatory approach to the public-private partnership in cybersecurity. In 2002, Congress enacted the Protected Critical Infrastructure Information Program (PCII) "to protect private sector information voluntarily shared with the government for the purposes of homeland security."[59] Under this program, DHS has been given procedures for receiving, validating, handling, storing, marking, and using information voluntarily shared by industry.[60] Perhaps most importantly to the PPP aspect of the PCII Programs, PCII information cannot be disclosed through a FOIA request, in civil litigation, or for additional regulatory purposes.[61]

Additionally, in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015, which "created a framework to foster greater information-sharing in both directions: industry-to-government and government-to-industry. The framework envisioned in CISA is:

> *A voluntary cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information… [and allow] for greater cooperation and collaboration in the face of growing cybersecurity threats to national and economic security.*[62]

Pursuant to CISA, the Cyber Information and Collaboration Program ("CISCP") at DHS is the focal point for data sharing and analytical collaboration. The goal of CISCP is "to establish

---

[58] See Brown, "Cyber Imperative," pgs. 7-8.
[59] DHS, CISA Protected Critical Infrastructure Information Program ("PCII"), https://www.cisa.gov/pcii-program, accessed October 7, 2020.
[60] See Brown, "Cyber Imperative," pp. 12-14.
[61] Brown, "Cyber Imperative."
[62] Quoting Senate Rep. No. 114-32 (2015). https://www.congress.gov/congressional-report/114th-congress/senate-report/32/1, accessed October 7, 2020.

a community of trust between the Federal Government and entities from across the different critical infrastructure sectors and then leverage these relationships for enhanced information-sharing and collaboration."[63] For instance, the Financial Services Sector Coordination Council welcomed CISA as "a strong vote of confidence for information sharing and its importance as a key component of cyber risk mitigation."[64] Other commentators have stated that CISA has developed a "needed cyber security asset, and industry welcomed it to 'help business achieve timely and actionable situational awareness to improve detection, mitigation, and response capabilities against cyber threats.'"[65]

The main strength of the CISA approach is that it embraces the public-private partnerships' ability to empower private expertise to address evolving cyber threats by incentivizing corporations to protect their information systems, customer data, and networks; by allowing corporations (and other nongovernmental entities) who know their cyber infrastructure vulnerabilities to develop solutions to their own data security and cybersecurity challenges; and by being forward-looking to adapt to challenges or rapidly changing technology."[66] For instance, when the Game Over Zeus botnet emerged, the DHS and FBI were able to work closely with the financial and business actors to disable a botnet which was "believed to be responsible for the theft of millions of dollars from business

---

[63] DHS. Cyber Information Sharing and Collaboration Programs (CISCP) (June 2013), https://csrc.nist.gov/CSRC/media/Events/ISPAB-JUNE-2013-MEETING/documents/ispab_june2013_menna_ciscp_one_pager.pdf, accessed October 7, 2020.

[64] Id. Similarly, DOD has also acknowledged "a maturation of the relationship between government and private sector DIB partners." See. Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, Preface, p. iii, https://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf, accessed October 8, 2020.

[65] Brown, Cyber Imperative, p. 8. See also, DHS, Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program. https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf, accessed October 8, 2020.

[66] Brown, "Cyber Imperative, p. 8.
FBI, Game Over Zeus Botnet Disrupted, Collaborative Effect Among International Partners (June 2, 2014, updated July 11, 2014), https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted, accessed October 8, 2020.

and consumers in the U.S. and around the world."[67] The response to the Game Over Zeus botnet attack represents a substantial improvement to the lack of coordinated action taken by Sony and government/law enforcement following the Sony Pictures attack in 2014.

In order to bolster incentives for public-private cybersecurity partnerships, policymakers need to continue to reduce barriers to private participation. This can be done by the following: 1) providing the same level of protection for private-to-private information-sharing as private-to-government sharing; 2) expanding CISA protections from purely defensive measures to the development of all best practices cybersecurity strategies; 3) strengthening CISA's antitrust exemptions to encourage business-to-business information-sharing; 4) expanding exemptions from Freedom of Information Act ("FOIA") requests under CISA beyond trade secrets and proprietary information; and 5) adding additional safe harbor and immunity provisions to CISA in troublesome areas, such as tort claims, class action suits, and SEC securities disclosure actions.[68] Protecting the private sector from the apparent downsides to private sector collaboration/cooperation in the PPP will encourage broader information-sharing, development of best practices, and greater cooperation with federal and state and local governments to address cybersecurity challenges in real time, and thus, hopefully, will allow closer to real-time responses to cyber threats, such as the North Korean attack on Sony Pictures.[69]

The Trump Administration's National Cyber Strategy represents a positive, if less than fully-detailed, advancement of

[67] Brown, Cyber Imperative, pp. 12-13. See also, DHS, Strategic Principles for Securing the Internet of Things (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf, accessed October 8, 2020.
[68] Brown, Cyber Imperative.
[69] See, U.S. Department of State, Recommendation to the President on Deterring Adversaries and Better Protecting the American People from Cyber Attacks (May 31, 2018), https://www.state.gov/recommendations-to-the-president-on-deterring-adversaries-and-better-protecting-the-american-people-from-cyber-threats/, accessed October 8, 2020.

the historic U.S. public-private partnership in the cybersecurity based on an improved supply-chain; use of best practices, and rapid responses to real-time threats. The Trump Cyber Strategy uses free market ideas; best practices; and coordination, cooperation, and information-sharing techniques to attempt to advance the public-private partnership in cybersecurity. It needs to address more specifically some of the potential incentives and liabilities to the private sector for participation in this partnership. The Trump Cyber Strategy, along with the use of ISACs, CISA, and the newly-independent Cybersecurity and Information Security Agency, should advance the U.S. national security interest by allowing for more rapid response to cyber espionage incursions and physical cyber attacks in real time.

However, the challenges posed by the myriad and rapidly-evolving challenges of cybersecurity are great. The issue of cyberespionage is still a troublesome one, in no small part because cyber espionage often results in greater geopolitical and economic risks, as the Chinese hacking of OMB showed. The dangers of cyber attacks resulting in physical damage to critical infrastructure in defense, intelligence, and critical infrastructure are still great and require a firm "red line" and deterrence by denial strategy, as David Sanger has advocated, particularly in the most critical areas of national security, such as the defense/industrial base, the intelligence community, and the electric grid. Other "critical" aspects of the nation's infrastructure, such as transportation, telecommunications, and IT, will have to rely on closer real-time coordinated responses with DHS. Perhaps, most significantly, cyber manipulation of democratic processes and elections in the U.S. and abroad via the use of Facebook, Google, and Twitter requires an even deeper dive into the nature of public-private partnership on public information-sharing platforms (and greater awareness by the American public of the information and data they are consuming and the effects it is having on them) in order to re-enforce and strengthen U.S. democratic processes and institutions.

An Evaluation of the Economic Espionage Act 18 U.S. Code § 1831

Michael Eddi

This paper seeks to examine the technicalities that limit the Economic Espionage Act (EEA) and offer policy recommendations for enhancing its practicality and bolstering its usefulness as a tool to fight economic espionage found to be committed against the United States. The ideas presented in this essay come at a crucial time when forward thinking regarding the issue of how best to tackle and prosecute the known attempts at stealing U.S. trade secrets continues to puzzle Intelligence Community officials and lawmakers alike.

Crimes of industrial espionage have become some of the biggest threats to American national security in the 21st century and often result in failed litigation. Corporate America and smaller private firms that develop unique and original trade secrets require bolstered laws and stronger educational programs that assist in the defense against intellectual property (IP) theft. Additionally, the government must ensure that the U.S. intelligence community is equipped with the proper legal tools to promote the successful prosecution of those guilty of economic espionage. To achieve these goals, I propose three main policy options: primarily, the legal departments within the Department of Justice (DOJ) should be merged to cut down the number of department filters through which economic espionage cases pass; second, amendments should be made to the language of section 6001 of the IRTPA and

incorporated into the EEA; third, there should be an issuance of another organizational amendment that establishes a primary point of contact/bureau within the U.S. State Department's Intellectual Property Enforcement (IPE) office that private attorneys could contact for help when representing clients in international IP cases.

The EEA falls under title 18 of the U.S. Code and is therefore a criminal statute. The law states that, in general terms, economic espionage is "the unlawful or clandestine targeting or acquisition of sensitive financial, trade or economic policy information; proprietary economic information; or technological information."[1] Formally, The Economic Espionage Act of 1996 (EEA), 18 U.S.C. §§ 1831-1839, "defines the term 'economic espionage' as the theft or misappropriation of a trade secret with the intent or knowledge that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."[2] The act of receiving, purchasing, or possessing a trade secret known to have been stolen or misappropriated, as well as any attempt or conspiracy to commit economic espionage, is punishable as a federal crime under the EEA.[3]

Because the Economic Espionage Act falls under title 18 of the U.S. federal code, it leaves no room for private action to be taken by U.S. citizens/corporations against those accused of intellectual property theft. This means that private corporations seeking to pursue litigation/prosecution against the accused IP thief must first appeal to the Federal Bureau of Investigation (FBI) to open an inquiry into the matter and then convince a federal prosecutor that there is a case to be tried in the first place.[4] Hedi Nasheri, a senior research fellow at New

---

[1] 18 U.S.C. § 1831. *Economic espionage*. 2019. Cornell Law School Legal Information Institute, https://www.law.cornell.edu/wex/economic_espionage#:~:text=The%20Economic%20Espionage%20Act%20of,foreign%20instrumentality%2C%20or%20foreign%20agent., accessed October 8, 2020.

[2] Ibid.

[3] Ibid.

[4] Nasheri, Hedi. *The Challenge of Economic Espionage.* 2012.

York University's Law School Center for Research in Crime and Justice, further explains that "[…] as a general rule, U.S. attorneys' offices are not set up to prosecute violations of the EEA in the same manner in which, for example, they routinely prosecute drug or gun crimes. Not only that, federal regulations require that EEA prosecutions be cleared by the Justice Department in Washington. Specifically, prosecutions for foreign-related thefts must be approved by the Computer Crime and Intellectual Property Section of the Criminal Division, while domestic-only cases must be approved by the Internal Security Section before indictments may be issued."[5] Nasheri's apt analysis reveals that there is perhaps a bureaucratic structural overcomplication hindering our federal prosecutor's willingness and ability to effectively employ the EEA.

However, it is in our best interest to explore options that cut down on the number of department filters that economic espionage cases need to go through before indictments can be issued. To remedy this situation, the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division responsible for cases pertaining to economic espionage ought to be integrated into the National Security Division (NSD) of the Department of Justice. Although the EEA is criminal in nature, the ethos of economic espionage cases lend themselves to the work of the IC and are thus better aligned with the primary mission of the NSD which is, "To protect the United States from threats to our national security by pursuing justice through the law."[6]

Alternatively, the CCIPS could be merged with the Litigation Section (LS) within the NSD. The LS "reviews and prepares requests for Attorney General authorization to use [Foreign Intelligence Surveillance Act] (FISA) information in criminal

[5] Nasheri, Hedi. "The Challenge of Economic Espionage." June 5, 2012, *World Politics Review*. https://www.worldpoliticsreview.com/articles/12025/the-challenge-of-economic-espionage, accessed October 8, 2020.
[6] United States Department of Justice, About the Division, https://www.justice.gov/nsd/about-division, accessed October 8, 2020.

and non-criminal proceedings."[7] The section also drafts motions and briefs and responds to defense motions to disclose FISA applications and to suppress the fruits of FISA collection. Finally, the section works to ensure the consistent application of FISA in trial and appellate courts nationwide. To support this effort, the NSD in January 2008 developed a new policy, which was "… Approved by the Attorney General, for investigators and prosecutors on the use of information obtained or derived from FISA collections."[8] Merging the CCIPS with a section which is heavily involved in FISA carries great advantages that could very well bolster the efficiency and evidence-gathering power of the newly combined sections, and may result in a higher number of full penalty prosecutions per economic espionage trial, thus making it a stronger deterrent to nefarious activity of this nature.

Delving further into FISA, the language found in section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458 could be amended and incorporated into economic espionage law that would allow the FBI to employ FISA with greater ease in cases pertaining to industrial espionage. Specifically, this section amended the definition of an "Agent of a foreign power" in FISA, 50 U.S.C. § 1801(b)(1), to add a new class of covered individuals. Under the new "lone wolf" provision, "… a non-United States person who engages in international terrorism or activities in preparation for international terrorism is deemed to be an 'agent of a foreign power under FISA."[9] Moreover, it is important to understand that "The […] provision does not change the procedures to be used to apply for a court order authorizing electronic surveillance or a physical search under FISA. If an order is sought under this definition of an 'agent of a foreign power,' however, the applicant is not required to

[7] United States Department of Justice, Sections and Offices, https://www.justice.gov/nsd/sections-offices, accessed October 8, 2020.
[8] Ibid.
[9] Bazan, Elizabeth B. "Intelligence Reform and Terrorism Prevention Act of 2004: 'Lone Wolf' Amendment to the Foreign Intelligence Surveillance Act," 2004, https://fas.org/irp/crs/RS22011.pdf, accessed October 8, 2020.

demonstrate a connection between the target of the electronic surveillance or physical search and a foreign nation, foreign group, or international terrorist group. Nor does the Foreign Intelligence Surveillance Court (FISC), in approving such an order, have to find probable cause to believe that such a connection existed. Rather, if the court authorizes such a surveillance or physical search using this new definition of 'agent of a foreign power,' the FISC judge has to find, in pertinent part, that, based upon the information provided by the applicant for the order, the target had engaged in or was engaging in international terrorism or activities in preparation therefor."[10] Simply stated, if the amendment is not renewed at its sunset clause date on March 15th, 2020[11], then the standard for obtaining FISA orders will revert back to necessitating probable cause, which is a higher burden of proof, showing the person to be acting on behalf of a particular entity engaged in international terrorism, or in this case, economic espionage.[12]

Unfortunately, there are limited viable solutions or propagable amendments that would allow corporations and individual entities to pursue independent prosecution against IP thieves. However, it may be possible, from a federal perspective, to incorporate language from the Justice Against Sponsors of Terrorism Act (JASTA) that could possibly allow private citizens to pursue independent action against foreign agents engaged in economic espionage. In its inception, the JASTA act stated that U.S. citizens were permitted to sue a foreign state if such state was designated as a state sponsor of terrorism by the United States Department of State and if they were harmed by that state's aid for international terrorism.[13] JASTA authorizes

[10] Ibid.
[11] https://docs.house.gov/billsthisweek/20191118/BILLS-116HR3055SA-RCP116-38.pdf. SEC. 1703. Sunsets
[12] Chesney, Robert. "Three FISA Authorities Sunset in December: Here's What You Need to Know" January 16, 2019, Lawfare, https://www.lawfareblog.com/three-fisa-authorities-sunset-december-heres-what-you-need-know, accessed October 8, 2020.
[13] Pub. L. 114-222 Justice Against Sponsors of Terrorism Act, https://www.congress.gov/114/plaws/publ222/PLAW-114publ222.htm, accessed October 8, 2020.

federal courts to exercise subject matter jurisdiction over any foreign state's support for acts of international terrorism against a U.S. national or property regardless of whether such state is designated as a state sponsor of terrorism or not.[14] This section of the act could be reworded to state that U.S. citizens are permitted to sue a foreign state, or foreign agent, if it is found that said foreign state, or agent, was discovered to be conducting and or supporting actions that are, or are perceived to be, pertaining to the conduct of economic/industrial espionage activities against U.S. businesses operating domestically or abroad by the U.S. Department of State; furthermore, U.S. citizens would be permitted to sue said actors if they were harmed by their attempts at economic/industrial espionage.

This new definition would provide statutory justification for private action at the behest of privately owned corporations in criminal cases brought against states or individuals suspected of economic or industrial espionage. Additionally, "The practical effect of the [original] legislation was to allow the continuation of a longstanding civil lawsuit brought by the families of victims of the September 11 attacks against Saudi Arabia for its government's alleged role in the attacks."[15] This same rationale can be applied to the EEA, as it would again allow those harmed by economic or industrial espionage to pursue civil lawsuits against foreign agents or actors discovered to be conducting economic/industrial espionage against U.S. businesses operating domestically or abroad. Concomitantly, it is critical to acknowledge that the original JASTA act *does not* identify Saudi Arabia by name, as identifying another country in federal legal matters could have massive diplomatic and international relations implications. Therefore, any amendments made to the EEA to include language of this

[14] Ibid.
[15] United States Congress. S.2040 – Justice Against Sponsors of Terrorism Act, https://www.congress.gov/bill/114th-congress/senate-bill/2040/text, accessed October 8, 2020.

nature should follow suit and remain ambiguous so as not to blatantly target or identify any one nation in particular.

Prospects of enforcing the penalties associated with economic espionage are another matter entirely and remain low, as there are few ways of enforcing legal matters in countries like China, which has proven to be the biggest threat to American trade secrets today. Paul Chan, the Managing Principal and a trial lawyer at Bird Marella in Los Angeles, writes that, "Although China is a member of the Hague Convention, requests to serve a resident of mainland China with legal process must be coordinated through China's Central Authority, and efforts by the Chinese authorities to perfect service of process in China are not dependable. U.S. courts therefore lack power to reliably compel the appearance or participation of Chinese residents in U.S. legal proceedings. And historically, U.S. civil judgments have not been enforceable in China. Given these significant limitations in the enforcement and collection of private money judgments, it would not be unreasonable to expect that private litigants contemplating the costs of cross-border litigation, without the resources of the U.S. government at their backing, will necessarily be more selective in deciding what types of civil litigation to pursue against Chinese adversaries."[16]

For example, Dan Harris, founder of the Harris Bricken international law firm, confirms that there are only a handful of viable ways for private citizens to approach trademark and IP theft when dealing with China. Non-usage clauses and legal workarounds are among the go-to responses for many lawyers dealing with clients embroiled in these cases. However, if all else fails, the final legal option available to private litigants is an attempt to purchase their trademark and IP back from the

[16] Chan, Paul S. "The Rise in Economic Espionage Cases Involving China," May 9. 2019, Bloomberg Law, https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-the-rise-in-economic-espionage-cases-involving-china, accessed October 8, 2020.

company that stole it.[17] Unfortunately, Harris explains that this tends to be tougher and more expensive than one likely would expect. Litigants must facilitate these purchases by obtaining a Chinese citizen (not a lawyer or anyone with any apparent connection to the law firm) residing in China to facilitate the negotiations.[18] Avoiding suspicions of American involvement in the negotiations is key, as any such hints would signal that the law firm is operating for an American company. Exposure of this knowledge to the Chinese thief corporation would then, in turn, exponentially increase the amount of money required for a company to reclaim the trademark in question.[19] It may make more sense to establish a company in Hong Kong to conduct the process, due to the fact that "…The Hague options available to an individual in cases pertaining to Hong Kong are more varied, but considerably faster, easier, and more likely to lead to an enforceable judgment."[20,21]

The process for filing a case through The Hague Convention in China requires strict adherence to Article 5 stipulations. All requests coming through China's central authority must follow the subsequent steps, beginning with filing a Hague Evidence Request. The side pursuing litigation must absorb the cost, which may be substantial, to fully translate all relevant documents pertaining to the case. According to China's declaration to Article 5(3), "…Although the defendant may speak flawless English, omitting translated documents will prompt the Central Authority to reject a request. And for [the sake of clarity] get the right written form of Chinese, which is simplified."[22] Additionally, if the defendant is a company, it would be wise to "Hire an investigator to ascertain the

[17] Harris, Dan. "China Trademark Theft. It's Baaaaaack in a Big Way," August 16, 2018, China Law Blog, https://www.chinalawblog.com/2018/08/china-trademark-theft-its-baaaaaack-in-a-big-way.html, accessed October 8, 2020.
[18] Ibid.
[19] Ibid.
[20] Lukken, Aaron. "How to Serve Process in China," January 12, 2017, Hague Law Blog, https://www.haguelawblog.com/2017/01/serve-process-china/, accessed October 8, 2020.
[21] Harris, Dan. *China Trademark Theft. It's Baaaaaack in a Big Way*, 2018.
[22] Lukken, Aaron. *How to Serve Process in China*. 2017.

appropriate address for service. It may not appear anywhere in the documents that have already been exchanged, and if the wrong address is provided, the Central Authority can reject the request. […] In any of these circumstances, the case will be rejected and thrown away."[23] Moreover, if it is a U.S. action, then, "The party pursuing litigation must wire $95 to the Central Authority. The Convention arguably prohibits the assessment of fees, but the United States charges $95, so China returns the favor on a reciprocal basis."[24] Lastly, the party pursuing litigation must fill out a USM-94 completely and ensure that it is signed by a court official, attorney, or person that is commissioned to do so by the court.[25]

After considering the lengthy process that a citizen or corporation must go through to pursue action against a Chinese party, it would be wise to issue another organizational amendment, in addition to moving the CCID to the LS, to establish a primary point of contact/bureau within the U.S. State Department's Intellectual Property Enforcement (IPE) office that private attorneys can contact for help when representing clients in international IP cases. As it stands, the IPE works with the Bureau of International Narcotics and Law Enforcement (INL) through "the International Computer Hacking and Intellectual Property (ICHIP) program. ICHIPs are experienced DOJ attorneys placed at U.S. embassies in key regions to enhance foreign law enforcement partner capacity to investigate and prosecute IPR crimes."[26] Additionally, the IPE maintains an IP Attaché program. The IPE Team "works with the United States Patent and Trademark Offices to place the IP Attachés at several embassies and consulates. IP Attachés are technical experts who work to improve IP systems internationally. The Attachés advocate to improve IP policies, laws, and regulations abroad for the benefit of U.S. businesses

[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] U.S. State Department, IP Enforcement Abroad, https://www.state.gov/intellectual-property-enforcement/ip-enforcement-abroad/, accessed October 8, 2020.

and stakeholders."[27] This program could double as an effective tool to inform and teach U.S. business owners about best practices when it comes to economic espionage and IP security in the workplace. The Attaché would also be an invaluable consultation resource for U.S. attorneys and provide an excellent non-legal option for combating economic espionage through passive educational and non-provocative/accusatory means.

Intellectual property theft has become a large-scale threat to U.S. national security in 2020. The legal means laid out in this paper by which the U.S. can explore new and creative ways to combat/mitigate the effects of IP theft and economic espionage are predicated on the assumption that new language can/will be added to existing laws and statutes. These amendments would ultimately allow for easier prosecution of those who commit economic espionage against the U.S. Additionally, it is imperative that organizational and structural changes be made to the American bureaucracy to allow for the removal of the proverbial red tape which prevents or discourages economic espionage cases from ever being brought to trial in the first place. Lastly, we must continue to bolster the educational and professional resources available to private citizens and non-federal attorneys so we can attack the issue of economic espionage from a self-help standpoint.

[27] Ibid.