# Plan Texts

Plan: The Department of the Treasury's Office of Foreign Assets Control should use its licensing authority and enforcement discretion to exempt transactions from enforcement under the Cuban Assets Control Regulations as they pertain to information and communication technology investment in the Republic of Cuba.

# Inherency

#### Previous reforms failed- depoliticized investment in ICT infrastructure is key

Piccone et al 10 (Theodore J. Piccone, Christopher Sabatini and Carlos Saladrigas. July 15th, 2010, “Bridging Cuba’s Communication Divide: How U.S. Policy Can Help”

<http://www.brookings.edu/~/media/events/2010/7/15%20cuba%20communications/07_cuba_telecommunications_piccone.pdf> Accessed: 9/3/12 MB)

It is unreasonable to hope for the development of other ICTs, such as the internet and social media, without economic models to make them work. Thus, the challenge for U.S. policymakers consists not only in effecting targeted reforms to its 50-year old embargo, but in broadly lifting all restrictions that hinder the development of an economic model capable of sustaining the requisite investments in ICT in Cuba, and the corresponding consumer demand for the services. A piecemeal approach will simply not do the job. Laying this knowledge and infrastructure foundation is essential for the long-term economic prospects of the Cuban people. Getting there requires three steps: 1) more explicit and flexible U.S. regulations governing the export and investments in ICT infrastructure in Cuba; 2) more flexible U.S. regulations to allow for the development of an ICT consumer market in Cuba; and 3) the development of distance-learning programs on the technology, experiences and applications of ICT to economic In April 13, 2009, President Obama took the first step in what many hoped would be a steady stream of initiatives to unlock the door to U.S.-Cuban relations, frozen for 50 years by intransigence on both sides of the Florida straits. Among the modest measures announced, the White House said it wanted to “promote contacts between Cuban-Americans and their relatives in Cuba” and “increase the flow of information to the Cuban people” by authorizing U.S. telecommunications companies to provide certain and humanitarian activity services to customers in Cuba. Five months later, the regulations released by the Administration in order to implement the President’s directive on telecommunications were met by many businesses with deafening silence and scratched heads. Why? The technical answer is that the new rules fail to give service providers the clear guidance they need to enter the icy waters of U.S.-Cuban commerce. They also fail to facilitate the creation of the necessary economic models to sustain the investment and infrastructure needed to modernize Cuba’s ICT system. But the political answer to industry’s chilly reception may lie in the President’s explicit linkage between liberalizing ICT regulations and the overarching goal to promote democracy and human rights, “decrease the dependency of the Cuban people on the Castro regime and to encourage positive change in Cuba.” By, in effect, tasking the U.S. telecommunications industry with the difficult though laudable job of promoting democracy and human rights in Cuba, the Administration may have made the environment too “political” and therefore less hospitable for U.S. investors. This is not to excuse in any way the Cuban regime’s ongoing denial of its citizens’ basic rights to free expression. As a signatory to the International Covenant on Civil and Political Rights, which guarantees the right “to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice,” the Cuban government certainly should abide by its international obligations by liberalizing trade and services in modern telecommunications, the oxygen any polity needs to develop and govern itself today. But in the context of ongoing hostilities between Washington and Havana, overt U.S. demands for political change on the island inevitably are exploited as another stone in David’s sling against Goliath. There is an alternative approach to resolving this dilemma. Another longstanding U.S. policy goal, articulated both rhetorically and in such legislation as the Cuban Democracy Act of 1992, 22 U.S.C. 6001, is to support the Cuban people in their daily struggles to cope with the deprivations of life in a closed authoritarian regime. Facilitating contact within families is certainly one way to ease the strain of separation among loved ones, both on and off the island. To that end, U.S. law allows, inter alia, the sale and donations of food, the export of medicines and medical supplies, and the provision of telecommunications facilities “in such quantity and of such quality as may be necessary to provide efficient and adequate telecommunications services between the United States and Cuba.” 22 U.S.C. 6004. In other words, Congress has already authorized transactions that permit the kind of “efficient and adequate” ICT services that we take for granted today. Taken from this perspective, and given the telecommunications revolution since the Act was passed, it is clear that U.S. policy should dramatically expand the availability of modern information and communication services to the Cuban people. The Obama administration can support the Cuban people’s basic quality of life and their right to information by rewriting its regulations to allow the sale of all types of ICT equipment and permit U.S. investments in ICT, including mobile devices and fiber optic cables; reducing the red tape of case-by-case licensing; and lifting restrictions, especially on financial transactions, that limit consumer spending on ICT and the ability of ordinary Cubans to engage in ecommerce, thus helping to lessen individual citizens’ dependency on the state.

# Advantage one is China

#### Cuba is key- proximity gives China the ability to intercept US messages

Simmons 12 (Chris, June 11, 2012 , Chris Simmons a retired Counter-intelligence Special Agent with 28 years service in the Army, Army Reserve, and the Defense Intelligence Agency, and has testified on the subject of Cuban espionage before members of U.S. House Foreign Affairs “Dirty Little Secret: Why China Needs Cuba” <http://cubaconfidential.wordpress.com/2012/06/11/dirty-little-secret-why-china-needs-cuba/> Accessed: 8/27/13 MB)

As China continues its quest to replace the U.S. as the world’s only superpower, spying remains a core means in fulfilling its economic, military, and political needs. The FBI has long considered China the greatest spy threat to the United States, based in part on the research of the U.S.-China Economic and Security Review Commission, which continues to perform an excellent job documenting the Chinese espionage threat (see http://www.uscc.gov/) French writer Roger Faligot, author of The Chinese Secret Service from Mao to the Olympics, contends more than two million people work for Chinese intelligence. For comparison, Dennis Blair, the former Director of National Intelligence, said 200,000 personnel serve in the U.S. Intelligence Community. His figure does not include foreign agents working for the United States. Functionally, most of China’s spies work, directly or indirectly, in espionage performed by agents and collaborators. Beijing’s second greatest espionage capability is stealing foreign communications – “Signals Intelligence” or SIGINT in spy parlance. While China maintains “the most extensive SIGINT capability of any nation” in Asia according to a U.S. government report, Beijing’s historical challenge has been the lack of direct access to satellite and radio downlinks going directly into the United States. Normally, gaining access to downlinks is relatively easy, as the signal coming towards earth spreads out into a huge cone covering hundreds, if not thousands of miles. However, the sheer volume of U.S. communications requires a vast number of satellite dishes and antennae arrays, making such a SIGINT effort impossible to hide. As a result, China proved unable to collect against most U.S. communications until the late 1990s, when Havana provided it access to the regime’s major SIGINT sites. Cuba’s location places it in the downlink of dozens of U.S. government and commercial signals. From an espionage standpoint, nowhere else in the Western Hemisphere provides a better site to conduct unrestricted SIGINT operations. Headquartered at Bejucal, just west of Havana, the SIGINT effort run by Cuba’s Directorate of Military Intelligence (DIM) involves roughly 1000-1,200 personnel. Defectors claim Havana also operates covert SIGINT sites in its Washington-based Interests Section and in its diplomatic facility at the United Nations. These covert sites provide unique access to localized communications. Defectors and émigrés also report for at least 20 years, the DIM has collected more SIGINT than it can analyze. According to think tanks, Cuban émigrés, and the media, Chinese military SIGINT personnel have served at Bejucal and a sister site at Santiago de Cuba since at least 1999. There, U.S. military communications as well as financial and political information is collected and analyzed by an elite Cuban-Chinese military team. In exchange for U.S. secrets, China appears to provide Havana with weaponry, updated SIGINT equipment, intelligence training, and money. Moscow proved the unique role Cuba can play in SIGINT targeting of the United States. For nearly 40 years, it ran a massive SIGINT complex at Lourdes, near Cuba’s Bejucal facility. However, the 28-square mile facility became a political liability and economic drain on Moscow after the Cold War. In 2001, Russia closed it and removed its 1000-1500 personnel. In contrast, China avoided risking any political and economic costs of its SIGINT endeavor by embedding its staff in Cuban facilities. This commingling has also made Beijing’s presence significantly smaller and less visible, providing China plausible deniability about its role.

#### Two scenarios-

#### First is military power

Huawei has the capability to cut off all US military communications

O’Connor, Huntley, and Kalister 13 (Nicholas C., Wade Huntley, Linda Kalister March, 2013 .Naval Postgraduate School. Senior lecturer in the National Security Affairs department at the Naval Postgraduate School. Independent consultant on international security issues. Previously was Director of the Simons Centre for Disarmament and Non-Proliferation Research at the University of British Columbia in Vancouver. Kalister is an Analyst at DoD and Defense Intelligence Agency. “THE LONG-TERM U.S. STRATEGIC IMPLICATIONS OF HUAWEI’S PENETRATION IN LATIN AMERICA”

<http://calhoun.nps.edu/public/bitstream/handle/10945/32876/13Mar_O'Connor_Nicholas.pdf?sequence=1> Accessed: 8/26/13 MB)

While Huawei has purportedly been very successful at illegally using its equipment and access to collect information, it has been surrounded by controversy. In recent years, the most glaring controversy in the U.S. is the suspicion of espionage. In February 2011, Huawei wrote a letter to the United States to address these concerns. “We sincerely hope that the United States government will carry out a formal investigation on any concerns it may have about Huawei” (Hu 2011, 5). The U.S. accepted this invitation. The House Permanent Select Committee on Intelligence initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States (Rogers and Ruppersberger 2012, iv). One of the main focuses of the investigation was the suspicion of espionage. “Chinese actors are the world’s most active and persistent perpetrators of economic espionage” (Foreign Spies Stealing US Economic Secrets in Cyberspace 2011, 5). These concerns about China led to similar suspicions of Huawei. The Committee spent a significant amount of time looking into these suspicions, and the connections between Huawei and the Chinese 3 government made up a large part of the investigative report. There are many ways in which a telecommunications company could conduct espionage. One way that this could be conducted is through the insertion of foreign devices into its telecommunications equipment. Malicious hardware or software could allow the Chinese government to shut down or degrade critical national security systems in a time of crisis (Rogers and Ruppersberger 2012, 3). This is one of the biggest reasons that officials do not want Huawei to expand into the Latin America or the U.S. In addition to inserting hardware and software, Huawei could also use its personnel to conduct espionage. An example of this would be inserting a spy into Huawei’s team of engineers. “To identify and resolve the issues, they will gain full access to network architecture and design - a security risk for network reconnaissance” (Ferro 2012, under "The security risk is the team of engineers"). This would be the case in any country in which Huawei installed the infrastructure. If Huawei was to conduct such an operation, this would allow for easy reconnaissance. “As an attacker, knowing weak points, physical locations, logical layouts, what the target response plan is, and what equipment is all just marvellous intelligence” (Ferro 2012, under "What Security Actions are Possible"). All of these could potentially be gained by someone posing as an engineer or support technician. These are threats that should be concerning to nations hosting Huawei infrastructure in Latin America.4 Not only is Latin America close to the United States geographically, but the U.S. maintains close relations with many of these countries. In addition, the U.S. military conducts operations in Latin America. The U.S. operates over twenty military bases throughout Latin America (Whitney Jr. 2012, para. 1). An attack on the infrastructure there could have serious impact on military communications.

#### That kills heg- a cyberattack shuts down the entire economy and decimates the military

Wolter 13 (Rachel, March 1st, 2013, master's degree from the University of Massachusetts Boston in Public Affairs and International Relations. Master's of Science in International Relations with a focus on Chinese foreign policy. “China Hackers Could Neutralize U.S. Defenses With a Few Button Clicks”

<http://www.policymic.com/articles/28295/china-hackers-could-neutralize-u-s-defenses-with-a-few-button-clicks> Accessed 9/4/13 MB)

The United States is heavily dependent on information technology for defense and military purposes, banking, and transportation as well as to deliver power, fuel and water across the country; therefore, America is highly vulnerable to cyber attacks. According to Shawn Henry of the Federal Bureau of Investigation, "cyber threats are an existential one, meaning that a major cyber attack could potentially wipe out whole companies. It could shut down our electric grid or water supply. It could cause serious damage to parts of our cities, and ultimately even kill people." China is targeting our most vulnerable points: infrastructure, communication networks, and defense technology. Big guns and large militaries no longer determine a nation-state’s ability to win a war. As the world’s reliance on global commerce and information technology increases, cyber power is the new variable in determining the power of state rather than nuclear arsenals that characterized the Cold War. Beijing is well aware of this fact and knows China cannot compete with the military power of the United States. Cyberspace allows China to easily and repeatedly attack the United States from abroad. Militaries and their equipment, economies, financial operations and domestic infrastructures can become paralyzed once a nation-state’s digital infrastructure is compromised, rendering an all-powerful military useless. Just like in Live for or Die Hard, China can systematically shut down all of the computer networks, satellites, and defense capabilities of the United States with a few codes and mouse clicks. While China may not be attempting to bring Washington to their knees, cyber attacks are part of every militaries' weapons arsenal. In the event a mishap over Taiwan occurs or U.S. Navy boats in the South China Sea become hostile, leading to conflict, breeching networks and communication systems could neutralize the U.S. military giving China a greater chance of winning a war against the United States.

#### U.S. hegemonic decline causes global great-power war

Zhang, Carnegie Endowment for International Peace researcher & Shi, World Bank consultant, 11

(Yuhan Zhang, researcher at the Carnegie Endowment for International Peace; Lin Shi, Columbia University, independent consultant for the Eurasia Group and consultant for the World Bank, January 22, 2011, “America’s decline: A harbinger of conflict and rivalry,” East Asia Forum, online: http://www.eastasiaforum.org/2011/01/22/americas-decline-a-harbinger-of-conflict-and-rivalry/, accessed 6/27/12, THW)

Over the past two decades, no other state has had the ability to seriously challenge the US military. Under these circumstances, motivated by both opportunity and fear, many actors have bandwagoned with US hegemony and accepted a subordinate role. Canada, most of Western Europe, India, Japan, South Korea, Australia, Singapore and the Philippines have all joined the US, creating a status quo that has tended to mute great power conflicts. However, as the hegemony that drew these powers together withers, so will the pulling power behind the US alliance. The result will be an international order where power is more diffuse, American interests and influence can be more readily challenged, and conflicts or wars may be harder to avoid. As history attests, power decline and redistribution result in military confrontation. For example, in the late 19th century America’s emergence as a regional power saw it launch its first overseas war of conquest towards Spain. By the turn of the 20th century, accompanying the increase in US power and waning of British power, the American Navy had begun to challenge the notion that Britain ‘rules the waves.’ Such a notion would eventually see the US attain the status of sole guardians of the Western Hemisphere’s security to become the order-creating Leviathan shaping the international system with democracy and rule of law. Defining this US-centred system are three key characteristics: enforcement of property rights, constraints on the actions of powerful individuals and groups and some degree of equal opportunities for broad segments of society. As a result of such political stability, free markets, liberal trade and flexible financial mechanisms have appeared. And, with this, many countries have sought opportunities to enter this system, proliferating stable and cooperative relations. However, what will happen to these advances as America’s influence declines? Given that America’s authority, although sullied at times, has benefited people across much of Latin America, Central and Eastern Europe, the Balkans, as well as parts of Africa and, quite extensively, Asia, the answer to this question could affect global society in a profoundly detrimental way. Public imagination and academia have anticipated that a post-hegemonic world would return to the problems of the 1930s: regional blocs, trade conflicts and strategic rivalry. Furthermore, multilateral institutions such as the IMF, the World Bank or the WTO might give way to regional organisations. For example, Europe and East Asia would each step forward to fill the vacuum left by Washington’s withering leadership to pursue their own visions of regional political and economic orders. Free markets would become more politicised — and, well, less free — and major powers would compete for supremacy. Additionally, such power plays have historically possessed a zero-sum element. In the late 1960s and 1970s, US economic power declined relative to the rise of the Japanese and Western European economies, with the US dollar also becoming less attractive. And, as American power eroded, so did international regimes (such as the Bretton Woods System in 1973). A world without American hegemony is one where great power wars re-emerge, the liberal international system is supplanted by an authoritarian one, and trade protectionism devolves into restrictive, anti-globalisation barriers. This, at least, is one possibility we can forecast in a future that will inevitably be devoid of unrivalled US primacy.

#### Heg is inevitable and sustainable but ONLY with economic and military strength

Kagan 12 [Robert Kagan, Senior Fellow at the Brookings Institute, B.A., Yale University, M.P.P., John F. Kennedy School of Government, Harvard University, Ph.D., American University, January 17, 2012, “Not Fade Away: Against the Myth of American Decline”, Brookings Institute, <http://www.brookings.edu/research/opinions/2012/01/17-us-power-kagan>, DMintz]

Less than a decade ago, most observers spoke not of America’s decline but of its enduring primacy. In 2002, the historian Paul Kennedy, who in the late 1980s had written a much-discussed book on “the rise and fall of the great powers,” America included, declared that never in history had there been such a great “disparity of power” as between the United States and the rest of the world. Ikenberry agreed that “no other great power” had held “such formidable advantages in military, economic, technological, cultural, or political capabilities.... The preeminence of American power” was “unprecedented.” In 2004, the pundit Fareed Zakaria described the United States as enjoying a “comprehensive uni-polarity” unlike anything seen since Rome. But a mere four years later Zakaria was writing about the “post-American world” and “the rise of the rest,” and Kennedy was discoursing again upon the inevitability of American decline. Did the fundamentals of America’s relative power shift so dramatically in just a few short years?¶ The answer is no. Let’s start with the basic indicators. In economic terms, and even despite the current years of recession and slow growth, America’s position in the world has not changed. Its share of the world’s GDP has held remarkably steady, not only over the past decade but over the past four decades. In 1969, the United States produced roughly a quarter of the world’s economic output. Today it still produces roughly a quarter, and it remains not only the largest but also the richest economy in the world. People are rightly mesmerized by the rise of China, India, and other Asian nations whose share of the global economy has been climbing steadily, but this has so far come almost entirely at the expense of Europe and Japan, which have had a declining share of the global economy.¶ Optimists about China’s development predict that it will overtake the United States as the largest economy in the world sometime in the next two decades. This could mean that the United States will face an increasing challenge to its economic position in the future. But the sheer size of an economy is not by itself a good measure of overall power within the international system. If it were, then early nineteenth-century China, with what was then the world’s largest economy, would have been the predominant power instead of the prostrate victim of smaller European nations. Even if China does reach this pinnacle again—and Chinese leaders face significant obstacles to sustaining the country’s growth indefinitely—it will still remain far behind both the United States and Europe in terms of per capita GDP.¶ Military capacity matters, too, as early nineteenth-century China learned and Chinese leaders know today. As Yan Xuetong recently noted, “military strength underpins hegemony.” Here the United States remains unmatched. It is far and away the most powerful nation the world has ever known, and there has been no decline in America’s relative military capacity—at least not yet. Americans currently spend less than $600 billion a year on defense, more than the rest of the other great powers combined. (This figure does not include the deployment in Iraq, which is ending, or the combat forces in Afghanistan, which are likely to diminish steadily over the next couple of years.) They do so, moreover, while consuming a little less than 4 percent of GDP annually—a higher percentage than the other great powers, but in historical terms lower than the 10 percent of GDP that the United States spent on defense in the mid-1950s and the 7 percent it spent in the late 1980s. The superior expenditures underestimate America’s actual superiority in military capability. American land and air forces are equipped with the most advanced weaponry, and are the most experienced in actual combat. They would defeat any competitor in a head-to-head battle. American naval power remains predominant in every region of the world.¶ By these military and economic measures, at least, the United States today is not remotely like Britain circa 1900, when that empire’s relative decline began to become apparent. It is more like Britain circa 1870, when the empire was at the

#### Second is US-Sino War

#### Uncertainty surrounding cyber attacks ensures miscalculation and retaliation- that escalates

Eaves 13 (David, March 12, 2013, Master’s of International Relations at Oxford. Former Sauvé Scholar at McGill University. Program Director for the Code for America Institute. Works with the Harvard Negotiation Project.“Cyberwarfare's "Cuban Missile Crisis" Moment” <http://techpresident.com/news/23599/cyberwarfares-cuban-missile-crisis-moment> Accessed: 9/2/13 MB)

The United States and China seem poised to begin negotiations around the militarization of the Internet, and just in time — because the uncertainty surrounding what might be proportional response to an attack over the Internet, and a dearth of international agreement around what has already become a venue for hostilities, puts international relations in far more precarious a position than many might realize. The recent publicity around cyberattacks on the United States — especially those blamed on China — have moved the issue of "cybersecurity" to the mainstream. It might not be immediately obvious why we should care — but we should. Isn't this just a continuation of the games nations play? Same as it ever was? Maybe. But there is a real risk that increased connectivity of the world is changing the nature of the threat — with serious implications for peace and stability. This would certainly not be the first time technology altered a balance of military power and destabilized global political orders everyone thought was robust. One reason the world plunged into global war in 1914 after a relatively minor terrorist attack — the assassination of Arch-Duke Ferdinand — was because the hot new technology of the day, the speedy railway, caused strategists to believe it would confer a decisive advantage on those who mobilized first. The advent of nuclear intercontinental ballistic missiles of the 1950s had a similar effect, with fears that a first strike "decapitation attack" against Moscow from Turkey, or against Washington from Cuba, could preempt a counter attack. Cyber warfare may be evolving into a similarly destabilizing type of technology. Prior to the 21st century, cyber attacks were relatively localized affairs. People imagined the main threats of a cyber attack being with virtual thefts from banks, identify theft against individuals and even industrial piracy. Serious problems to be sure, but not end-of-the-world stuff. Even when targeted against the state, cyber attacks rarely pose an existential threat to a country. The loss of state secrets, the compromising of some officials could, cumulatively, be corrosive on a state's ability to defend itself or advance its interests, but it was unlikely even a combination of operations would shake a mature state to its core. Two things have changed. First, as cyberspace has grown its networked nature has altered the potential scale and reach of cyber-attacks. The ability to take a country's critical infrastructure offline, or worse, turn it against its owners, creates the possibility that it could pose an existential threat in the same way nuclear weapons did — but with complexity added because the country under attack won't be easily able to pinpoint the source of the threat. The threats of a cyber attack are becoming more significant. Second, the potential impact of an attack are increasing in magnitude but the consequences have not become clear. Bruce Schneier — who is very much worth reading and will likely disagree with this piece — may be right that most cyber "attacks" are really just acts of espionage, but there is not a clear line between espionage and warfare. At some point the potential size and scale of the act moves it out of the former category and into the latter. Here, other forms of warfare there have evolved a set of norms, a sort of code of conduct, between states. However frightening, these codes of conduct — often a series of escalating maneuvers to show one is serious about protecting one's interests — are nonetheless stabilizing since it gives the whole system some predictability and thus stability. And herein lies the problem. There is no accepted norm for how to deal with a cyber attack. Indeed there isn't even an accepted definition of what constitutes a cyber-attack. Consequently it may be getting harder and harder to predict a state's response to an attack. This could introduce an enormous amount of uncertainty into the international system — uncertainty that can make it easier to miscalculate a target's reaction to cyber attack with potentially deadly consequences.

#### US- China war is the most likely extinction scenario

Wittner 11 ( Lawrence S., 10/29/11, Emeritus Professor of History at the State University of New York/Albany “Is a Nuclear War with China Possible?” http://www.huntingtonnews.net/14446)

But what would that victory entail? A nuclear attack by China would immediately slaughter at least 10 million Americans in a great storm of blast and fire, while leaving many more dying horribly of sickness and radiation poisoning. The Chinese death toll in a nuclear war would be far higher. Both nations would be reduced to smoldering, radioactive wastelands. Also, radioactive debris sent aloft by the nuclear explosions would blot out the sun and bring on a nuclear winter around the globe destroying agriculture, creating worldwide famine, and generating chaos and destruction.¶ Moreover, in another decade the extent of this catastrophe would be far worse. The Chinese government is currently expanding its nuclear arsenal, and by the year 2020 it is expected to more than double its number of nuclear weapons that can hit the United States. The U.S. government, in turn, has plans to spend hundreds of billions of dollars modernizing its nuclear weapons and nuclear production facilitate ties over the next decade.¶ To avert the enormous disaster of a U.S.-China nuclear war, there are two obvious actions that can be taken. The first is to get rid of nuclear weapons, as the nuclear powers have agreed to do but thus far have resisted doing. The second, conducted while the nuclear disarmament process is occurring, is to improve U.S.-China relations. If the American and Chinese people are interested in ensuring their survival and that of the world, they should be working to encourage these policies.¶

#### Now is key- recent tech developments make US cyberdefenses weak

Lieberthal and Singer 12 (Kenneth and Peter, February 2012, director of the John L. Thornton China Center and senior fellow in Foreign Policy and Global Economy and Development at Brookings. Singer is Director of the 21st Century Defense Initiative and a senior fellow in Foreign Policy Served on the National Security Council. “Cybersecurity and U.S.-China Relations” <http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf> Accessed: 8/30/13 MB)

Offense has the advantage. In any issue of security, there is a premium on defending oneself to make attack less effective and potentially creating some form of deterrence to dissuade future attacks. The challenge in the cyber security domain is that the one seeking to penetrate a computer network, at least so far, is at a great advantage relative to the defender. At its most basic level, the Internet was designed to share information easily, not prevent its flow. Similarly, most of the products and systems that link into this network of networks were not designed with security embedded into them. Rather, there are many vulnerabilities that can be exploited. Moreover, even the very manner of updating and “patching” security vulnerabilities relies on the ready flow of information to let users know about new risks and how to fix them. Many feel that this trend will only continue, with the relative advantage of the offense in the cyber realm growing further. The technical tools for penetration and extraction without (or at least before) detection continue to improve exponentially. Even more, the tools exist now for turning other electronic devices that people have in proximity to their computer networks into espionage platforms. Keylogger technology, for example, can be used to remotely track the buttons one uses on the keyboard through malware inside the computer. Other malware may remotely turn on the camera and microphone of a computer or other device in a room to monitor what is happening.47 In Oct. 2011, it was revealed that such malware had even penetrated the supposedly secure networks used to control U.S. military drones.48 Passwords are, moreover, increasingly vulnerable. Technology to break passwords has reached the point that most passwords other than very sophisticated “highly secure” ones can be compromised by those with the available advanced tools.49 In addition, at some administrative level in networked organizations, there are one or more files that contain the passwords of everyone who uses that network—and those files can themselves be compromised. More broadly, the sophistication of approaches to gaining unapproved access is increasing more rapidly and effectively than is generally appreciated. A particularly worrisome change in the environment of cybersecurity has been the rise of what are known as “advanced persistent threats,” or APTs. Rather than the randomized, quick hit attacks of the past, in an APT operation a specific individual or organization is identified by a group, and the sort of complex resources and techniques traditionally used by espionage professionals are used to go after the targeted network over an extended period of time. An APT features teams of professionals with varied skill sets (intelligence gathering, infiltration, exfiltration, etc.) working together. The target’s internal organization, chain of command, norms of behavior, and even social dynamics are studied and mapped out to figure out who matters and who does not and what key vulnerabilities can be compromised. Social networking, in particular, has allowed people to share more and more about themselves online. But it has also created enormous new sources of detailed data on individuals that is used, in turn, to develop pathways and strategies to penetrate computer networks to which those individuals—or their online “friends” or friends of friends—have access.50 In sum, while there are cyber defenses that are very sophisticated and fairly widely deployed, it is usually more challenging to prevent, and even detect, malicious activity of a sophisticated nature. Indeed, even the defense method of “air-gapping” one’s computer networks has not proved to be a remedy. The Iranian facilities hampered by Stuxnet were not directly connected to the Internet but still had malware enter them (probably by naïve individuals bringing across software physically).51 The same has happened on multiple occasions to U.S. defense networks, in one case when users literally plugged in memory sticks they had found in a parking lot (thought to have been distributed by a foreign intelligence organization) into computers on classified networks.52 Constant efforts are needed, therefore, to build user awareness, upgrade defensive capabilities, and ascertain what data has been lost or compromised. But a basic reality of cyber security at this point is to accept the cold hard fact that the defense is at a disadvantage. It is telling that even the vaunted U.S. National Security Agency, arguably the most sophisticated entity in the world at cyber issues, operates on the assumption that its networks are compromised—but most other agencies and users around the world do not.53

#### Removing telecom sanctions removes China’s competitive advantage in Cuba

Stratfor 1 ("China: Huawei's massive US connections" Global Intelligence Update, March 20, 2001. www.atimes.com/china/CC21Ad02.html) VP

Huawei is a prime example of this new dynamic. Huawei is an emerging global powerhouse with powerful internal backers and strong global alliances. A former officer of the People's Liberation Army, Ren Zhengfei, founded the company in 1988 as a reseller of imported telecommunications equipment. The company quickly began producing its own branded telecom and information technology equipment. Huawei's 1999 net profits of US$182 million made it China's most profitable telecom equipment company. ¶ The company has benefited from powerful connections. The PLA remains a steady customer and - by some accounts - is more intimately involved with the company. Another key supporter is Beijing, which in 1996 introduced a policy to support domestic telecom companies in the face of foreign competition. Huawei was designated a "key development project" by the Shenzhen government. State-sponsored credit poured into the company. The government also expedited company issues through China's vast bureaucracy, extended generous credit to Huawei's customers and lent the company large sums for research and development. ¶ This allowed Huawei to consolidate its domestic business and move aggressively into foreign markets. Huawei targeted emerging markets where China has long-standing relationships and where competition from the dominant global players is more limited. Some countries that fall into this category - Myanmar, Cuba, Iraq, Iran, Libya and Sudan - are considered pariah states in the United States and represent sources of potential conflict similar to the current Iraq/Huawei case. ¶ Huawei employed its strategy effectively, gaining market share in Russia and portions of Eastern Europe and Africa. Huawei is now competing with the likes of Cisco and Lucent, recently beating out both for a contract to supply equipment to Thailand's second-largest Internet service provider. ¶ American firms might be tempted to support sanctions on the company as a means of undercutting an emerging competitor. But American firms, recognizing Huawei offers access into lucrative Chinese telecom and data communications markets as well as into the rest of Asia, prefer to engage Huawei and will likely resist attempts to sanction the company. ¶ China is the fastest growing communications market in the world outside the United States. Cooperating with Huawei ingratiates foreign companies to Beijing and can help them meet local content requirements for manufacturing facilities. ¶ The list of American companies aggressively courting Huawei include 3Com, AT&T, Cisco, IBM, Intel, Lucent and Motorola. IBM signed an agreement last September to be Huawei's primary supplier of processors and chips for the company's routers and switches. The deal should add about 10 percent to IBM's worldwide network processing equipment revenues, according to Computerwire. Motorola signed an agreement last year to purchase Huawei mobile communications equipment for its Chinese base stations. ¶ American firms are developing vital relationships and facing new competition, which affects their global business strategies. This will lead to greater resistance to a hard-line policy on China or sanctions on its firms. And American sanctions on countries like Cuba and Iraq giving Chinese competitors an advantage in emerging markets could increase pressure on the Bush administration to abandon sanctions.

#### Permitting US companies in Cuba allows them to control the market

Bloomberg 1/26/11 (“Chavez Beats AT&T to Cuban Telecom `Gold Mine' as Dispute on Pricing Bites” http://www.bloomberg.com/news/2011-01-26/chavez-beats-at-t-to-cuba-telecom-market-as-price-dispute-bites.html)

U.S. companies had been backing a separate venture by Miami-based TeleCuba CommunicationsInc, which said it was granted a license to build a 110-mile link from Key West, Florida, to Havana after President Barack Obama in 2009 loosened the U.S. trade embargo for phone service providers. The project has been delayed over the Federal Communications Commission’s refusal to accept price demands by President Raul Castro’s government for routing calls. “This is a huge missed opportunity,” said Chris Sabatini, senior policy director at the New York-based Council of the Americas, a business group. “If you can get into a market early on, you can control it all along the value chain.” Cuba’s population of 11.4 million could become the largest telecom market in the Caribbean, topping Puerto Rico’s $1.6 billion market, according to Pyramid Research in Cambridge, Massachusetts. Even if the market remains mostly closed, annual revenue could still reach $400 million by 2013 from the current $80 million, Pyramid said.

#### Now is key- ZTE and Huawei are on the brink

Morgon 13 [Micheal, ABI Researcher, August 21, Fierce Wireless, “Analyzing the world's 14 biggest handset makers in Q2 2013”, <http://www.fiercewireless.com/europe/special-reports/analyzing-worlds-14-biggest-handset-makers-q2-2013#ixzz2eMOq2VU>, accessed 9/7, CC]

Despite a drop in handset and smartphone shipments in Q2, ZTE was able to increase its penetration of smartphone shipments to 75%. Like other Chinese OEMs, ZTE felt the pressure of Samsung in its key home market of China. ZTE is expected to continue to push itself up the value chain from low-cost handsets into premium smartphones and further develop its brand strength and recognition. While upmarket movement is a classic strategy, ABI Research believes that ZTE should not move up stream at the expense of its core strength in delivering low-cost products. Huawei faced a shipment decline in Q2 from seasonality and increasing competition from both the high and the low end. While Huawei does have increasing presence in international markets and in particular emerging smartphone markets, it will be increasingly important that it defends its position in China. ABI Research beleives that if Huawei's inherent advantages in China cannot hold against Samsung's marketing budget, there will be little to stop Samsung from pushing Huawei back in other developed markets such as West Europe and North America. Furthermore, if Huawei cannot hold its share against the likes of Coolpad and Xiaomi, Huawei will be in a very tight spot.

# Advantage 2 is OFAC

#### OFAC is overstretched—the plan is key to effective sanctions

Johnson, Spector and Lilac 10 - Andy Johnson, Director, National Security Program, Kyle Spector, Policy Advisor, National Security Program, Kristina Lilac, National Security Program, Senior Fellows of The Third Way Institute, (“End the Embargo of Cuba”, Article for The Third Way Institute, 9/16/10, <http://content.thirdway.org/publications/326/Third_Way_Memo_-_End_the_Embargo_of_Cuba.pdf>, Accessed 7/02/13)

Keeping the embargo in place requires that the US government devote time and resources to fighting a Cold War -8 era threat. Senator Chris Dodd argued in a 2005 op ed that the US spends “extraordinary resources” each year to enforce the sanctions instead of devoting such resources to the fight against terrorism. 4 While the financial resources dedicated to enforcing the embargo may be limited compared to resources dedicated to other causes, lifting the Cuban embargo could put the US in a better position to fight terrorist organizations by freeing up resources currently enforcing the embargo. For example, the Treasury Department’s Office of Foreign Assets Control (OFAC), which governs travel and trade between the US and Cuba, is also responsible for maintaining sanctions against truly problematic countries, including Iran and North Korea. OFAC also is responsible for responding to economic threats posed by terrorist organizations and narcotics traffickers. By ending OFAC’s need to regulate the Cuban embargo, OFAC could instead devote those resources to respond to the current threats posed by rogue states and terrorist networks

#### **That revamps sanctions on Iran – previous lack of focus and disorganization**

Maberry and Jensen 13 – J. Scott Maberry, J.D, Georgetown University Law Center, International Trade partner in the Government Contracts, Investigations & International Trade Practice Group, Mark L. Jensen, J.D, Harvard Law School, International Trade associate in the Government Contracts, Investigations & International Trade Practice Group, (“OFAC gets hot, bothered on Iran and Cuba: how economic sanctions work today”, Report for Sheppard Mullin Richter & Hampton LLP, 5/7/13, <http://www.lexology.com/library/detail.aspx?g=8657e6ce-454a-4eaf-ba8b-d225ea59ecdd>, Accessed 7/9/13)

People who practice U.S. economic sanctions law like to talk about how sanctions are policy-oriented, or an engine of U.S. foreign policy. Whereas some laws may be more opaquely political, economic sanctions and embargoes seem to express most bluntly how international leverage works through regulation. And yet, a few recent regulatory developments show that the direction that sanctions take is not always predictable. The U.S. Department of Treasury, Office of Foreign Assets Control (“OFAC”) has had a raucously busy year. A torrent of development in laws and regulations on Iran served as the unsurprising focus of this year’s OFAC symposium, held on March 19, 2013, in Washington D.C. Among the developments were sanctions imposed on non-U.S. banks, a new executive order related to the purchase of petroleum and petrochemical products from Iran, an expanded scope of the Iran Transactions and Sanctions Regulations to companies “owned or controlled” by U.S. companies, and a new statute that targets sectors of the economy related to goods and services to Iran, including secondary financial transactions in energy, shipping, shipbuilding, precious metal, and graphite. See our recent posts on Iran here and here. Perhaps the most striking aspect of the Iran sanctions program is its proliferation into not only additional laws and regulations, but also additional regulatory regimes. The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (“CISADA”), the National Defense Authorization Act for 2012 (“NDAA”), and Iran Threat Reduction and Syria Human Rights Act of 2012 (“ITR”), have created a polyglot system focused on individual sectors of the economy. OFAC presenters at the March symposium gave the sense of a proliferation of laws that is undoubtedly aimed at accomplishing U.S. foreign policy goals. But the laws are paradoxically both targeted (at industries, vessels, banks) and incredibly expansive in jurisdiction. The system is the embodiment of the powerful yet somewhat disorganized U.S. government piling on everything it can to economically overwhelm Iran. The Iran program also serves as a good case study of how far and wide economic sanctions can be made to reach. If legislation of past years has proved anything, it is that the U.S. Congress appears ready to use any and all means within its legislative authority to sanction Iran. Insofar as Congress is able to map out the reach of the U.S. financial system and economy further, it seems likely that additional sanctions will be applied.

#### Iran already has capabilities for a bomb – only increasing sanctions can solve for increasing nuclear capabilities

Albright et al., Master of Science at Wright State University, 13

(David Albright, Mark Dubowitz, Orde Kittrie, Leonard Spector, Michael Yaffe, “The Project on U.S. Middle East Nonproliferation Strategy”, January 2013, accessed 9/17/13, http://isis-online.org/uploads/isis-reports/documents/FinalReport.pdf)

Given the progress that Tehran has already made with its nuclear plans—still-hidden centrifuge manufacturing plants, enrichment facilities at Natanz and Fordow, a likely, now sanitized weaponization facility at Parchin, and an extensive ballistic-missile program—the regime faces a short, relatively inexpensive dash to the nuclear finish line should it choose to take this step. According to a 2011 report by The Washington Post, IAEA officials have concluded that Iran has sufficient technical know-how to design and produce a functioning nuclear implosion device.41 Such a device would be usable in an underground nuclear explosion or for crude delivery (e.g., transportation by truck, ship, or aircraft). Iran would need more time to make a reliable warhead for a ballistic missile. A 2012 report by the Institute for Science and International Security states that, should Iran choose to do so, it could pursue one of several strategies that would allow it to develop a nuclear weapon. The probability of Iran’s pursuing such a strategy is judged to be medium in 2013.42 There is considerable debate regarding at what stage Iran’s nuclear program would be so advanced that it would no longer be possible in a timely manner to detect Iran’s acquisition of sufficient weapon-grade uranium or plutonium for a nuclear bomb. For example, in his September 2012 speech to the United Nations, Israeli Prime Minister Benjamin Netanyahu described when he considers that the red line for a nuclear Iran would be reached: the spring or summer of 2013, when he estimates the regime will, “at current enrichment rates,” have enough 20 percent-enriched uranium to make one bomb.43 Netanyahu stated as follows: In the case of Iran’s nuclear plans to build a bomb…Iran has to go through three stages…[During] the second stage: they have to enrich enough medium enriched uranium…Now they are well into the second stage. By next spring, at most by next summer at current enrichment rates, they will have finished the medium enrichment and move on to the final stage…The red line should be drawn right here…Before Iran completes the second stage of nuclear enrichment necessary to make a bomb. Before Iran gets to a point where it’s a few months away or a few weeks away from amassing enough enriched uranium to make a nuclear weapon.44 Netanyahu explained that in his view, “the relevant question is not when Iran will get the bomb” but rather “at what stage can we no longer stop Iran from getting the bomb,” and thus “the red line must be drawn on Iran’s nuclear enrichment program because these enrichment facilities are the only nuclear installations that we can definitely see and credibly target. President Obama has also attached considerable significance to the stage at which Iran’s nuclear program would be sufficiently advanced that it would no longer be possible to in a timely manner detect that Iran is acquiring a nuclear bomb. In the final presidential debate of the 2012 campaign, President Obama said: The clock is ticking. We’re not going to allow Iran to perpetually engage in negotiations that lead nowhere. And I’ve been very clear to them, you know…we have a sense of when they would get breakout capacity, which means that we would not be able to intervene in time to stop their nuclear program, and that clock is ticking.46 Another of the administration’s most specific statements on this issue was the December 2011 declaration by Defense Secretary Leon Panetta that, “If they proceed and we get intelligence that they are proceeding with developing a nuclear weapon then we will take whatever steps necessary to stop it.”47 In September 2012, Panetta expressed confidence in the ability of U.S. intelligence assets to detect an Iranian effort to develop a nuclear weapon in time for the U.S. military to prevent its fruition, stating “we think we will have the opportunity once we know that they’ve made that decision, to take the action necessary to stop (the program)” and “we have the forces in place…to do what we have to do to try to stop them from developing nuclear weapons.”48 This report’s recommendations for how the U.S. government should publicly address the question of red lines or triggers for military action against Iran’s nuclear program are contained in the report’s section titled “Credible Threat of Military Action.” We address here the different question of a recommended time frame for the United States and its allies to impose maximal sanctions pressure on Iran. We recommend that the United States and its allies impose maximal sanctions pressure on Iran prior to Iran’s reaching the critical capability to produce enough weapongrade uranium (or sufficient separated plutonium) for one or more bombs before the production of such an amount can reasonably be expected to be detected by the IAEA or Western intelligence services. Our analysis focuses on the speed with which Iran could produce enough weapon-grade uranium (or sufficient separated plutonium) because once the regime acquires such fissile material, it becomes far more difficult to stop the program militarily

#### Now is key to preventing Iran and Middle Eastern proliferation

Kroenig, assistant professor of government at Georgetown University, 12

(Matthew Kroenig, January/February 2012, “Time to Strike Iran: Why a Strike is the Least Bad Option”, accessed 9/15/13, <http://people.reed.edu/~ahm/Courses/Reed-POL-422-2012-S1_NP/Syllabus/EReadings/10.2/10.2.Kroenig2012Time.pdf>, ST)

Years of international pressure have failed to halt Iran’s attempt to build a nuclear program. The Stuxnet computer worm, which attacked control systems in Iranian nuclear facilities, temporarily disrupted Tehran’s enrichment effort, but a report by the International Atomic Energy Agency this past May revealed that the targeted plants have fully recovered from the assault. And the latest IAEA findings on Iran, released in November, provided the most compelling evidence yet that the Islamic Republic has weathered sanctions and sabotage, allegedly testing nuclear triggering devices and redesigning its missiles to carry nuclear payloads. The Institute for Science and International Security, a nonprofit research institution, estimates that Iran could now produce its first nuclear weapon within six months of deciding to do so. Tehran’s plans to move sensitive nuclear operations into more secure facilities over the course of the coming year could reduce the window for effective military action even further. If Iran expels IAEA inspectors, begins enriching its stockpiles of uranium to weapons-grade levels of 90 percent, or installs advanced centrifuges at its uranium-enrichment facility in Qom, the United States must strike immediately or forfeit its last opportunity to prevent Iran from joining the nuclear club. By Matthew Kroenig January/February 2012, some states in the region are doubting U.S. resolve to stop the program and are shifting their allegiances to Tehran. Others have begun to discuss launching their own nuclear initiatives to counter a possible Iranian bomb. For those nations and the United States itself, the threat will only continue to grow as Tehran moves closer to its goal. A nuclear-armed Iran would immediately limit U.S. freedom of action in the Middle East. With atomic power behind it, Iran could threaten any U.S. political or military initiative in the Middle East with nuclear war, forcing Washington to think twice before acting in the region. Iran’s regional rivals, such as Saudi Arabia, would likely decide to acquire their own nuclear arsenals, sparking an arms race. To constrain its geopolitical rivals, Iran could choose to spur proliferation by transferring nuclear technology to its allies -- other countries and terrorist groups alike. Having the bomb would give Iran greater cover for conventional aggression and coercive diplomacy, and the battles between its terrorist proxies and Israel, for example, could escalate. And Iran and Israel lack nearly all the safeguards that helped the United States and the Soviet Union avoid a nuclear exchange during the Cold War -- secure second-strike capabilities, clear lines of communication, long flight times for ballistic missiles from one country to the other, and experience managing nuclear arsenals. To be sure, a nuclear armed Iran would not intentionally launch a suicidal nuclear war. But the volatile nuclear balance between Iran and Israel could easily spiral out of control as a crisis unfolds, resulting in a nuclear exchange between the two countries that could draw the United States in, as well. These security threats would require Washington to contain Tehran. Yet deterrence would come at a heavy price. To keep the Iranian threat at bay, the United States would need to deploy naval and ground units and potentially nuclear weapons across the Middle East, keeping a large force in the area for decades to come. Alongside those troops, the United States would have to permanently deploy significant intelligence assets to monitor any attempts by Iran to transfer its nuclear technology. And it would also need to devote perhaps billions of dollars to improving its allies’ capability to defend themselves. This might include helping Israel construct submarinelaunched ballistic missiles and hardened ballistic missile silos to ensure that it can maintain a secure secondstrike capability. Most of all, to make containment credible, the United States would need to extend its nuclear umbrella to its partners in the region, pledging to defend them with military force should Iran launch an attack. In other words, to contain a nuclear Iran, the United States would need to make a substantial investment of political and military capital to the Middle East in the midst of an economic crisis and at a time when it is attempting to shift its forces out of the region. Deterrence would come with enormous economic and geopolitical costs and would have to remain in place as long as Iran remained hostile to U.S. interests, which could mean decades or longer. Given the instability of the region, this effort might still fail, resulting in a war far more costly and destructive than the one that critics of a preemptive strike on Iran now hope to avoid

#### Status quo sanctions working but not sufficient

Albright et al., Master of Science at Wright State University, 13

(David Albright, Mark Dubowitz, Orde Kittrie, Leonard Spector, Michael Yaffe, “The Project on U.S. Middle East Nonproliferation Strategy”, January 2013, accessed 9/17/13, http://isis-online.org/uploads/isis-reports/documents/FinalReport.pdf)

Iran’s oil exports have been halved by economic sanctions, leaving the regime with around $50 billion in oil income in 2012, and $37 billion in projected 2013 oil revenues (assuming Iran continues to export 1 million barrels per day at $100 per barrel).50 The Iranian economy has taken a substantial hit from the oil export and other sanctions on Iran. After the rial lost nearly half of its value in a week in October 2012, Tehran began severely restricting access to dollars and euros.51 That’s a clear sign that sanctions are having a strong impact on the Iranian economy. But the currency restrictions also served as a warning sign: In all probability the regime is husbanding foreign exchange reserves, and preparing for a long ordeal. Since existing sanctions thus far have failed to persuade Iran’s leaders to curtail their nuclear program definitively, what additional sanctions steps should be taken prior to Iran’s reaching critical capability? There is no way to know whether the Iranian regime will ever relent in its nuclear ambitions. There is always the possibility that the regime will keep enriching notwithstanding a looming, or even actual, sanctions-induced economic collapse. For sanctions to be given every chance of succeeding, though, the working assumption must be that sufficiently severe economic pressure will cause, or contribute significantly to causing, the Iranian regime to relent. Economic pressure seems most likely to succeed if it reaches maximum strength at least six months before Iran could go nuclear. The psychological impact of the pressure will need time to ripple through Iran’s political system, and a regime just weeks away from achieving its nuclear objective seems more likely to try to push on through. How strong will such economic pressure need to be? Since at least 2009, Secretary of State Hillary Clinton has been threatening Iran with “crippling sanctions.”52 However, the sanctions on Iran are not yet crippling, and Iran has yet to bring its nuclear program into compliance with UN Security Council requirements. The United States must intensify sanctions until the impact is so severe—as Iran’s revenues shrink, its currency loses more of its value, and its hard-currency reserves plummet—that Iran’s leaders change course and curtail their nuclear program. The number of months left for the West to impose maximal economic pressure on Iran in time to persuade Iran to halt its nuclear weapons program depends, of course, on what red line is set and when Iran is projected to cross it. For example, as mentioned previously, Netanyahu declared in his September 2012 speech to the United Nations that the red line for a nuclear Iran would be reached in the spring or summer of 2013, when he estimates the regime will, “at current enrichment rates,” have enough 20 percent-enriched uranium to make one bomb. Maximum economic pressure would need to occur by February 2013 for the Iranian regime to feel its full impact even four months (let alone six months) before Netanyahu’s red line. If necessary, the 2013 NDAA (discussed further below) and previous U.S. sanctions laws, vigorously implemented, could provide the U.S. government with all the authority it needs to impose near-maximal pressure on Iran. Such vigorous implementation could commence immediately. Implementation also could be adjusted in light of any meaningful concessions by Iran.

#### Iran nuclearization causes extinction – Israel preemptive strikes, Middle Eastern instability, and Saudi Arabian nuclear response

Edelman et al., U.S. Undersecretary of Defense for Policy in 2005 to 2009, 11

(Eric S. Edelmen, Andrew F. Krepinevich, and Evan Braden Montgomery, “The Dangers of Nuclear Iran: The Limits of Containment”, January/February 2011, accessed 9/15/13, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CEkQFjAD&url=http%3A%2F%2Fwww.csbaonline.org%2F4Publications%2FPubLibrary%2FA.20101227.The_Dangers_of_a_N%2FA.20101227.The_Dangers_of_a_N.pdf&ei=lj02UoB-woKLAt3YgIgF&usg=AFQjCNGATJneFTswWWxqO6Qz3_m25ehV5g&sig2=idc6UocQTkHGJMX9PwkSDA&bvm=bv.52164340,d.cGE&cad=rja>, ST)

Given Israel’ s status as an assumed but undeclared nuclear weapons state, the most immediate consequence of Iran’ s crossing the nuclear threshold would be the emergence of an unstable bipolar nuclear competition in the Middle East. Given Israel’ s enormous quantitative and qualitative advantage in nuclear weapons—its arsenal is estimated to consist of anywhere from 100 to more than 200 warheads, possibly including thermonuclear weapons—Tehran might fear a disarming preventive or preemptive strike. During a crisis, then, the Iranian leadership might face a “use them or lose them” dilemma with respect to its nuclear weapons and resolve it by attacking ﬁrst. For their part, Israeli leaders might also be willing to strike ﬁrst, despite the enormous risks. Israel’ s small size means that even a few nuclear detonations on its soil would be devastating; Iran’ s former president Ali Akbar Hashemi Rafsanjani was exaggerating only slightly when he claimed that “ even one nuclear bomb inside Israel will destroy everything. “ Iran’s nuclear arsenal is likely to be small at ﬁrst and perhaps vulnerable to a preventive attack. Moreover, even if current and future Israeli missile defenses could not stop a full-scale premeditated attack by ballistic missiles, they might be effective against any retaliation Iran might launch if it were hit ﬁrst. And the willingness to execute a preventive or preemptive strike when confronting a serious threat is a deeply ingrained element of Israel’ s strategic culture, as Israel demonstrated in its attacks against Egypt in 1956 and 1967, against Iraq’ s nuclear program in 1981, and against a suspected Syrian nuclear site in 2007. On the one occasion that Israel absorbed the ﬁrst blow, in 1973, it came perilously close to defeat. In short, the early stages of an Iranian-Israeli nuclear competition would be unstable. Even if Iran and Israel managed to avoid a direct conﬂict, Iran’s nuclear weapons would remain a persistent source of instability in the Middle East. Tehran would almost certainly attempt to expand the size of its arsenal to enhance the survivability of its nuclear weapons. To that end, it would have a strong incentive to adopt the North Korean model of proliferation: negotiating with the international community while continuing to expand its stockpile. Tehran could also deﬂect international pressure to disarm by offering to relinquish its arsenal if Israel did so as well, exploiting the desire of U. S. President Barack Obama and other Western leaders to make progress toward a world without nuclear weapons. As Iran’ s arsenal became larger and its fear of retaliation declined, however, it might be increasingly willing to engage in more subtle but still dangerous forms of aggression, including heightened support for terrorist groups or coercive diplomacy. Meanwhile, if Iran acquires nuclear weapons, Israel might face internal and external pressures to abandon its posture of nuclear opacity, that is, its policy of refusing to conﬁrm or deny that it has nuclear weapons. Internal pressure would come from those who believe that declaring Israel’s arsenal is necessary to deter an attack by Iran. External pressure would come from those who view an Israeli declaration as the ﬁrst step toward regional nuclear disarmament. But if Israel did abandon its policy of nuclear opacity, cooperation between Israel and its Arab neighbors would be far more difficult, and a containment strategy against Iran would thus be more challenging to implement. Such a disclosure might also encourage other states in the region to pursue their own nuclear weapons programs. Although most of Israel’ s neighbors have been willing to accept its undeclared nuclear weapons program so far, the combination of a nuclear-armed Iran and an openly nuclear armed Israel could alter their calculations—due to a heightened sense of threat, desire for prestige, domestic pressure, or all three. The reports of the Congressional Commission on the Strategic Posture of the United States and the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, as well as other analyses, have highlighted the risk that a nuclear-armed Iran could trigger additional nuclear proliferation in the Middle East, even if Israel does not declare its own nuclear arsenal. Notably, Algeria, Bahrain, Egypt, Jordan, Saudi Arabia, Turkey, and the United Arab Emirates— all signatories to the Nuclear Nonproliferation Treaty (npt)—have recently announced or initiated nuclear energy programs. Although some of these states have legitimate economic rationales for pursuing nuclear power and although the low-enriched fuel used for power reactors cannot be used in nuclear weapons, these moves have been widely interpreted as hedges against a nuclear-armed Iran. The NPT does not bar states from developing the sensitive technology required to produce nuclear fuel on their own, that is, the capability to enrich natural uranium and separate plutonium from spent nuclear fuel. Yet enrichment and reprocessing can also be used to accumulate weapons-grade enriched uranium and plutonium—the very loophole that Iran has apparently exploited in pursuing a nuclear weapons capability. Developing nuclear weapons remains a slow, expensive, and difficult process, even for states with considerable economic resources, and especially if other nations try to constrain aspiring nuclear states’ access to critical materials and technology. Without external support, it is unlikely that any of these aspirants could develop a nuclear weapons capability within a decade. There is, however, at least one state that could receive signiﬁcant outside support: Saudi Arabia. And if it did, proliferation could accelerate throughout the region. Iran and Saudi Arabia have long been geopolitical and ideological rivals. Riyadh would face tremendous pressure to respond in some form to a nuclear-armed Iran, not only to deter Iranian coercion and subversion but also to preserve its sense that Saudi Arabia is the leading nation in the Muslim world. The Saudi government is already pursuing a nuclear power capability, which could be the ﬁrst step along a slow road to nuclear weapons development. And concerns persist that it might be able to accelerate its progress by exploiting its close ties to Pakistan. During the 1980s, in response to the use of missiles during the Iran-Iraq War and their growing proliferation throughout the region, Saudi Arabia acquired several dozen css-2 intermediate-range ballistic missiles from China. The Pakistani government reportedly brokered the deal, and it may have also offered to sell Saudi Arabia nuclear warheads for the css-2s, which are not accurate enough to deliver conventional warheads effectively. There are still rumors that Riyadh and Islamabad have had discussions involving nuclear weapons, nuclear technology, or security guarantees. This “Islamabad option” could develop in one of several different ways. Pakistan could sell operational nuclear weapons and delivery systems to Saudi Arabia, or it could provide the Saudis with the infrastructure, material, and technical support they need to produce nuclear weapons themselves within a matter of years, as opposed to a decade or longer. Not only has Pakistan provided such support in the past, but it is currently building two more heavy-water reactors for plutonium production and a second chemical reprocessing facility to extract plutonium from spent nuclear fuel. In other words, it might accumulate more ﬁssile material than it needs to maintain even a substantially expanded arsenal of its own. Alternatively, Pakistan might offer an extended deterrent guarantee to Saudi Arabia and deploy nuclear weapons, delivery systems, and troops on Saudi territory, a practice that the United States has employed for decades with its allies. This arrangement could be particularly appealing to both Saudi Arabia and Pakistan. It would allow the Saudis to argue that they are not violating the npt since they would not be acquiring their own nuclear weapons. And an extended deterrent from Pakistan might be preferable to one from the United States because stationing foreign Muslim forces on Saudi territory would not trigger the kind of popular opposition that would accompany the deployment of U. S. troops. Pakistan, for its part, would gain ﬁnancial beneﬁts and international clout by deploying nuclear weapons in Saudi Arabia, as well as strategic depth against its chief rival, India. The Islamabad option raises a host of difficult issues, perhaps the most worrisome being how India would respond. Would it target Pakistan’s weapons in Saudi Arabia with its own conventional or nuclear weapons? How would this expanded nuclear competition inﬂuence stability during a crisis in either the Middle East or South Asia? Regardless of India’ s reaction, any decision by the Saudi government to seek out nuclear weapons, by whatever means, would be highly destabilizing. It would increase the incentives of other nations in the Middle East to pursue nuclear weapons of their own. And it could increase their ability to do so by eroding the remaining barriers to nuclear proliferation: each additional state that acquires nuclear weapons weakens the nonproliferation regime, even if its particular method of acquisition only circumvents, rather than violates, the NPT. Were Saudi Arabia to acquire nuclear weapons, the Middle East would count three nuclear-armed states, and perhaps more before long. It is unclear how such an n-player competition would unfold because most analyses of nuclear deterrence are based on the U. S. Soviet rivalry during the Cold War. It seems likely, however, that the interaction among three or more nuclear-armed powers would be more prone to miscalculation and escalation than a bipolar competition. During the Cold War, the United States and the Soviet Union only needed to concern themselves with an attack from the other. Multipolar systems are generally considered to be less stable than bipolar systems because coalitions can shift quickly, upsetting the balance of power and creating incentives for an attack. More important, emerging nuclear powers in the Middle East might not take the costly steps necessary to preserve regional stability and avoid a nuclear exchange. For nuclear-armed states, the bedrock of deterrence is the knowledge that each side has a secure second-strike capability, so that no state can launch an attack with the expectation that it can wipe out its opponents’ forces and avoid a devastating retaliation. However, emerging nuclear powers might not invest in expensive but survivable capabilities such as hardened missile silos or submarine-based nuclear forces. Given this likely vulnerability, the close proximity of states in the Middle East, and the very short ﬂight times of ballistic missiles in the region, any new nuclear powers might be compelled to “ launch on warning” of an attack or even, during a crisis, to use their nuclear forces preemptively. Their governments might also delegate launch authority to lower-level commanders, heightening the possibility of miscalculation and escalation. Moreover, if early warning systems were not integrated into robust command-and-control systems, the risk of an unauthorized or accidental launch would increase further still. And without sophisticated early warning systems, a nuclear attack might be un-attributable or attributed incorrectly. That is, assuming that the leadership of a targeted state survived a ﬁrst strike, it might not be able to accurately determine which nation was responsible. And this uncertainty, when combined with the pressure to respond quickly, would create a signiﬁcant risk that it would retaliate against the wrong party, potentially triggering a regional nuclear war. Most existing nuclear powers have taken steps to protect their nuclear weapons from unauthorized use: from closely screening key personnel to developing technical safety measures, such as permissive action links, which require special codes before the weapons can be armed. Yet there is no guarantee that emerging nuclear powers would be willing or able to implement these measures, creating a signiﬁcant risk that their governments might lose control over the weapons or nuclear material and that non-state actors could gain access to these items. Some states might seek to mitigate threats to their nuclear arsenals; for instance, they might hide their weapons. In that case, however, a single intelligence compromise could leave their weapons vulnerable to attack or theft. Meanwhile, states outside the Middle East could also be a source of instability. Throughout the Cold War, the United States and the Soviet Union were engaged in a nuclear arms race that other nations were essentially powerless to inﬂuence. In a multipolar nuclear Middle East, other nuclear powers and states with advanced military technology could inﬂuence—for good or ill—the military competition within the region by selling or transferring technologies that most local actors lack today: solid-fuel rocket motors, enhanced missile-guidance systems, warhead miniaturization technology, early warning systems, air and missile defenses. Such transfers could stabilize a fragile nuclear balance if the emerging nuclear powers acquired more survivable arsenals as a result. But they could also be highly destabilizing. If, for example, an outside power sought to curry favor with a potential client state or gain inﬂuence with a prospective ally, it might share with that state the technology it needed to enhance the accuracy of its missiles and thereby increase its ability to launch a disarming ﬁrst strike against any adversary. The ability of existing nuclear powers and other technically advanced military states to shape the emerging nuclear competition in the Middle East could lead to a new Great Game, with unpredictable consequences.

#### **OFAC is unique – involves allied cooperation**

DoT 05 – United States Department of Treasury, (“OFAC”, Report Written for the Federal Financial Institutions Examination Council, June 2005, <http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/ofac_sec_frb.pdf>, Accessed 7/9/13, AW)

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under the President’s wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations; supervisory examination for BSA compliance is logically connected to the examination of a financial institution’s compliance with OFAC sanctions

#### OFAC effectively targets Iranian businesses supporting proliferation

Fitzpatrick 1/16

--- Mark Fitzpatrick directs the IISS Non-Proliferation and Disarmament Programme, International Institute for Strategic Studies (“US sanctions on Iran“, January 16, 2013, IISS, [www.iiss.org/~/media/Documents/.../US%20sanctions%20on%20Iran.pdf](http://www.iiss.org/~/media/Documents/.../US%20sanctions%20on%20Iran.pdf), accessed July 10, 2013, MY)

Financial institutions that provide financial support for the sensitive nuclear and missile programs are also targeted. As a derivative, OFAC can target entities that are owned or controlled by the main entities. Whereas the UN has designated only two Iranian banks, the US blacklist includes about two dozen. The aim is to target financial institutions involved in any way that Iran moves money to finance proliferation. ￼￼The 2011 CISADA provided authority to designate any bank that deals with designated Iranian banks. This is often said to be an extra-territorial application of US law. US officials describe it differently: if third-country banks deal with Iran banks that are involved in proliferation, the Treasury Department does not want US banks risking their own reputation by involved with them. In this way, the Treasury Dept protects the US financial system from taint by association with proliferation. Only two third-country banks, in Iraq and China, have been so designated for helping Iranian banks evade sanctions.

# Solvency

#### the aff solves via specific exemptions — OFAC has broad discretion over sanctions enforcement.

Golumbic and Ruff 13 — Court E. Golumbic, Managing Director and Global Anti-Money Laundering, Anti-Bribery and Government Sanctions Compliance Officer at Goldman Sachs & Co., Lecturer-in-Law at the University of Pennsylvania Law School, former Assistant United States Attorney with the United States Attorney's Office for the Southern District of New York, and Robert S. Ruff III, Associate in the Securities Litigation practice group at Weil, Gotshal & Manges LLP, 2013 (“Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions,” *North Carolina Journal of International Law & Commercial Regulation* (38 N.C.J. Int'l L. & Com. Reg. 729), Spring, Available Online to Subscribing Institutions via Lexis-Nexis)

2. Ability to Mitigate Collateral Damage

Because OFAC prefers to formulate its sanctions program broadly, its economic sanctions can affect the lives of unintended targets, such as ordinary citizens of foreign countries that have no influence in their sanctioned government. n347 The broad reach of U.S. sanctions can also unnecessarily put U.S. citizens and companies at a competitive disadvantage, undermine international support for the sanctions programs, and even undermine the policy objectives of the programs. n348 One way in which OFAC mitigates [\*792] the collateral damage of its holistic sanctions is by issuing licenses that permit U.S. citizens to export food and medical supplies n349 and provide humanitarian aid n350 to people in sanctioned countries. In an effort to avoid placing private enterprises at an unnecessary competitive disadvantage, which can damage U.S. influence internationally and U.S. interests as a whole, OFAC may also allow certain activities from an otherwise sanctioned country. n351 Additionally, OFAC issues licenses to avoid interfering with the legitimate activities of international and charitable organizations and to permit U.S. persons to participate in such organizations. n352 By licensing these types of activities and transactions, OFAC focuses its sanctions and the punitive consequences thereof, to the extent possible, on those in a position to produce the desired change, rather than on innocent civilians and businesses. n353

#### Cuba will say yes

Sabatini 10 – Christopher Sabatini is senior director of policy at the Americas Society/Council of the Americas and editor in chief of Americas Quarterly. (“Havana Calling”, July/August 2010, Foreign Policy, <http://www.foreignpolicy.com/articles/2010/07/15/havana_calling?page=0,0>)

Would the Cuban government allow this? Some things -- such as licensing for satellite radio and television -- would clearly challenge the regime's monopoly on information. Yet some telecommunication investments, like establishing roaming agreements with U.S. carriers, the government would likely view as a much needed source of revenue. As for authorizing the purchase of laptops, software, and mobile-phone handsets? Well, that's already in large part out of its control as the increase in blogging and tweeting has demonstrated. But the benefits for individual Cubans' access to technology (with all the economic implications) will outweigh the benefits to the government.

#### **OFAC solves the China advantage- past instances of targeted communications licenses.**

Piccone et al 10 (Theodore J. Piccone, Christopher Sabatini and Carlos Saladrigas. July 15th, 2010, “Bridging Cuba’s Communication Divide: How U.S. Policy Can Help”

<http://www.brookings.edu/~/media/events/2010/7/15%20cuba%20communications/07_cuba_telecommunications_piccone.pdf> Accessed: 9/3/12 MB)

In accordance with this directive, on September 3, 2009, the Treasury Department’s Office of Foreign Assets Control (OFAC) published changes to the Cuban Assets Control Regulations (CACR) authorizing, by general license, certain financial transactions necessary to expand telecommunications links with Cuba. On September 8, 2009, the Bureau of Industry and Security (BIS) at the Department of Commerce published changes to the Export Administration Regulations (EAR) revising existing licensing policy for certain telecommunications related exports to Cuba. Among other things, the new CACR and EAR regulations: • Authorized transactions by U.S. telecom service providers, under a general license, including payments for (1) the provision of telecommunications between the United States and Cuba; (2) the provision of satellite T.V. services to Cuba; and (3) entry into roaming service agreements with telecommunications service providers in Cuba. • Authorized persons subject to U.S. law to enter into, and make payments under, contracts (including contracts for cellular telephone services) with non-Cuban telecommunications providers for services provided to Cubans. Authorized transactions, under specific licenses, incident to the establishment of facilities to provide telecom services linking third countries to Cuba if they are necessary to provide efficient and adequate telecommunications services between the United States and Cuba.

#### Libya proves OFAC’s effectiveness and rapid response.

Golumbic and Ruff 13 — Court E. Golumbic, Managing Director and Global Anti-Money Laundering, Anti-Bribery and Government Sanctions Compliance Officer at Goldman Sachs & Co., Lecturer-in-Law at the University of Pennsylvania Law School, former Assistant United States Attorney with the United States Attorney's Office for the Southern District of New York, and Robert S. Ruff III, Associate in the Securities Litigation practice group at Weil, Gotshal & Manges LLP, 2013 (“Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions,” *North Carolina Journal of International Law & Commercial Regulation* (38 N.C.J. Int'l L. & Com. Reg. 729), Spring, Available Online to Subscribing Institutions via Lexis-Nexis)

The United States' use of economic sanctions in response to the 2011 Libyan civil war provides a more recent example of the use of general licenses to adapt to a rapidly evolving situation. n399 On February 25, 2011, President Obama signed Executive Order 13,566 (EO 13,566), which prohibited all dealings by U.S. persons in the assets of certain named members of the Muammar Gaddafi regime, any person that the Treasury Secretary designated, and generally all persons involved in the political oppression of the Libyan people. n400 Additionally, EO 13,566 froze the assets of and prohibited U.S. persons from transacting with the Government of Libya, its agencies and controlled entities, and the Central Bank of Libya. n401 In imposing these sanctions, however, the Obama administration understood that such broad measures could eventually become unnecessary and even harmful to a new Libyan government. n402 Thus, as is commonplace with U.S. sanctions, EO 13,566 authorized the Treasury Department to issue licenses as well as delist designated persons. n403

The broad Libya sanctions triggered a torrent of specific [\*802] license applications, many of which concerned the same acceptable practices. n404 Thus, OFAC initially used its licensing power to issue general licenses responding to the common issues addressed in the specific license applications it received. n405 These general licenses included authorizations of transactions with financial institutions controlled by the Libyan government but were organized under the laws of another country, n406 transactions involving the provision of goods and services to the Libyan government's diplomatic missions, n407 transactions for certain legal services, n408 and transactions incident to the normal operations of investment funds that had sanctioned persons as non-controlling minority investors. n409

As the Libya conflict abated and the Gaddafi regime became less of a threat to the Libyan people, OFAC issued numerous general licenses that restored normal economic relations between the United States and Libya. n410 Indeed, approximately one month after the commencement of NATO operations, n411 OFAC issued a general license permitting transactions related to certain oil, gas, and petroleum exports from Libya occurring under the auspices of the Transitional National Council of Libya (TNC), n412 a then- [\*803] emerging anti-Gaddafi group which France had recognized as the sole representative of the Libyan people. n413 In August 2011, to reconcile the United States' recognition of the TNC as the legitimate governing authority in Libya with the contemporary sanctions targeting the Libyan government, OFAC issued a license generally authorizing all transactions with the TNC. n414 Following the fall of Tripoli, moreover, OFAC licensed transactions with the Libyan government and central bank. n415 Finally, in December 2011, OFAC issued a general license freeing the remainder of those entities' assets. n416 While these general licenses reduced the force of the U.S. sanctions against Libya, EO 13,566 remains in place, and thus OFAC retains the flexibility to ratchet up its sanctions should a change in Libyan politics militate such action. n417

#### OFAC decisions are binding and final.

Golumbic and Ruff 13 — Court E. Golumbic, Managing Director and Global Anti-Money Laundering, Anti-Bribery and Government Sanctions Compliance Officer at Goldman Sachs & Co., Lecturer-in-Law at the University of Pennsylvania Law School, former Assistant United States Attorney with the United States Attorney's Office for the Southern District of New York, and Robert S. Ruff III, Associate in the Securities Litigation practice group at Weil, Gotshal & Manges LLP, 2013 (“Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions,” *North Carolina Journal of International Law & Commercial Regulation* (38 N.C.J. Int'l L. & Com. Reg. 729), Spring, Available Online to Subscribing Institutions via Lexis-Nexis)

Licensing decisions are "final agency actions," and OFAC's regulations do not provide for a formal appeals process. n312 It is [\*785] doubtful, moreover, that a formal appeals process would provide much recourse for denied applicants. The U.S. District Court for the District of Columbia has held that because OFAC has complete discretion over specific licensing decisions, "no justiciable standard" exists for evaluating such decisions. n313 Nonetheless, OFAC will reconsider an application for "good cause," such as where the applicant can demonstrate "changed circumstances" or "submit additional relevant evidence that was not previously made available to OFAC." n314 Additionally, the applicant may request that OFAC explain why it denied a specific license application. n315 OFAC's responses to such requests are often no more than a generic indication that the applicant's described activity does not comport with U.S. foreign policy. n316