# Inherency

Obama’s previous reforms of telecommunication were not enough- by emphasizing democracy promotion over trade, few companies volunteered

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’s proximity to U.S. means Chinese companies are able to intercept U.S. 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

Chinese companies have the ability to cut off all US military communications

O’Connor, et al 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.

#### Hegemony prevents multiple nuclear conflicts

Brooks et al 13

(Stephen, Associate Professor of Government at Dartmouth College, John Ikenberry is the Albert G. Milbank Professor of Politics and International Affairs at Princeton University in the Department of Politics and the Woodrow Wilson School of Public and International Affairs, William C. Wohlforth is the Daniel Webster Professor in the Department of Government at Dartmouth College “Don’t Come Home America: The Case Against Retrenchment,” International Security, Vol. 37, No. 3 (Winter 2012/13), pp. 7–51)

A core premise of deep engagement is that it prevents theemergence of a far more dangerous globalsecurityenvironment. For one thing, as noted above, theUnited States’ overseaspresence gives it theleverage to restrain partners from takingprovocative action. Perhaps more important, its core alliance commitments also deter states with aspirations to regional hegemony from contemplating expansion and make its partners more secure, reducing their incentive to adopt solutions to their security problems that threaten others and thus stoke security dilemmas. The contention that engaged U.S. power dampens thebalefuleffects of anarchy is consistent with influential variants of realist theory. Indeed, arguably the scariest portrayal of the war-prone world that would emerge absent the “American Pacifier” is provided in the works of John Mearsheimer, who forecasts dangerous multipolar regions replete with security competition, arms races, nuclear proliferation and associated preventive war temptations, regional rivalries, and even runs at regional hegemony and full-scale great power war. 72 How do retrenchment advocates, the bulk of whom are realists, discount this benefit? Their arguments are complicated, but two capture most of the variation: (1) U.S. security guarantees are not necessary to prevent dangerous rivalries and conflict in Eurasia; or (2) prevention of rivalry and conflict in Eurasia is not a U.S. interest. Each response is connected to a different theory or set of theories, which makes sense given that the whole debate hinges on a complex future counterfactual (what would happen to Eurasia’s security setting if the United States truly disengaged?). Although a certain answer is impossible, each of these responses is nonetheless a weaker argument for retrenchment than advocates acknowledge. The first response flows from defensive realism as well as other international relations theories that discount the conflict-generating potential of anarchy under contemporary conditions. 73 Defensive realists maintain that the high expected costs of territorial conquest, defense dominance, and an array of policies and practices that can be used credibly to signal benign intent, mean that Eurasia’s major states could manage regional multipolarity peacefully without the American pacifier. Retrenchment would be a bet on this scholarship, particularly in regions where the kinds of stabilizers that nonrealist theories point to—such as democratic governance or dense institutional linkages—are either absent or weakly present. There are three other major bodies of scholarship, however, that might give decisionmakers pause before making this bet. First is regional expertise. Needless to say, there is no consensus on the net security effects of U.S. withdrawal. Regarding each region, there are optimists and pessimists. Few experts expect a return of intense great power competition in a post-American Europe, but many doubt European governments will pay the political costs of increased EU defense cooperation and the budgetary costs of increasing military outlays. 74 The result might be a Europe that is incapable of securing itself from various threats that could be destabilizing within the region and beyond (e.g., a regional conflict akin to the 1990s Balkan wars), lacks capacity for global security missions in which U.S. leaders might want European participation, and is vulnerable to the influence of outside rising powers. What about the other parts of Eurasia where the United States has a substantial military presence? Regarding the Middle East, the balance begins to swing toward pessimists concerned that states currently backed by Washington— notably Israel, Egypt, and Saudi Arabia—might take actions upon U.S. retrenchment that would intensify security dilemmas. And concerning East Asia, pessimism regarding the region’s prospects without the American pacifier is pronounced. Arguably the principal concern expressed by area experts is that Japan and South Korea are likely to obtain a nuclear capacity and increase their military commitments, which could stoke a destabilizing reaction from China. It is notable that during the Cold War, both South Korea and Taiwan moved to obtain a nuclear weapons capacity and were only constrained from doing so by a still-engaged United States. 75 The second body of scholarship casting doubt on the bet on defensive realism’s sanguine portrayal is all of the research that undermines its conception of state preferences. Defensive realism’s optimism about what would happen if the United States retrenched is very much dependent on its particular—and highly restrictive—assumption about state preferences; once we relax this assumption, then much of its basis for optimism vanishes. Specifically, the prediction of post-American tranquility throughout Eurasia rests on the assumption that security is the only relevant state preference, with security defined narrowly in terms of protection from violent external attacks on the homeland. Under that assumption, the security problem is largely solved as soon as offense and defense are clearly distinguishable, and offense is extremely expensive relative to defense. Burgeoning research across the social and other sciences, however, undermines that core assumption: states have preferences not only for security but also for prestige, status, and other aims, and they engage in trade-offs among the various objectives. 76 In addition, they define security not just in terms of territorial protection but in view of many and varied milieu goals. It follows that even states that are relatively secure may nevertheless engage in highly competitive behavior. Empirical studies show that this is indeed sometimes the case. 77 In sum, a bet on a benign postretrenchment Eurasia is a bet that leaders of major countries will never allow these nonsecurity preferences to influence their strategic choices. To the degree that these bodies of scholarly knowledge have predictive leverage, U.S. retrenchment would result in a significant deterioration in the security environment in at least some of the world’s key regions. We have already mentioned the third, even more alarming body of scholarship. Offensive realism predicts that the withdrawal of the American pacifier will yield either a competitive regionalmultipolarity complete with associated insecurity, arms racing, crisis instability, nuclear proliferation, and the like, or bids for regional hegemony, which may be beyond the capacity of local great powers to contain (and which in any case would generate intensely competitive behavior, possibly including regional great power war). Hence it is unsurprising that retrenchment advocates are prone to focus on the second argument noted above: that avoiding wars and security dilemmas in the world’s core regions is not a U.S. national interest. Few doubt that the United States could survive the return of insecurity and conflict among Eurasian powers, but at what cost? Much of the work in this area has focused on the economic externalities of a renewed threat of insecurity and war, which we discuss below. Focusing on the pure security ramifications, there are two main reasons why decisionmakers may be rationally reluctant to run the retrenchment experiment. First, overall higher levels of conflict make the world a more dangerous place. Were Eurasia to return to higher levels of interstate military competition, one would see overall higher levels of military spending and innovation and a higher likelihood of competitive regionalproxy wars and arming of client states—all of which would be concerning, in part because it would promote a faster diffusion of military power away from the United States. Greater regional insecurity could well feed proliferation cascades, as states such as Egypt, Japan, South Korea, Taiwan, and Saudi Arabia all might choose to create nuclear forces. 78 It is unlikely that proliferation decisions by any of these actors would be the end of the game: they would likely generate pressure locally for more proliferation. Following Kenneth Waltz, many retrenchment advocates are proliferation optimists, assuming that nuclear deterrence solves the security problem. 79 Usually carried out in dyadic terms, the debate over the stability of proliferation changes as the numbers go up. Proliferation optimism rests on assumptions of rationality and narrow security preferences. In social science, however, such assumptions are inevitably probabilistic. Optimists assume that most states are led by rational leaders, most will overcome organizational problems and resist the temptation to preempt before feared neighbors nuclearize, and most pursue only security and are risk averse. Confidence in such probabilistic assumptions declines if the world were to move from nine to twenty, thirty, or forty nuclear states. In addition, many of the other dangers noted by analysts who are concerned about the destabilizing effects of nuclear proliferation—including the risk of accidents and the prospects that some new nuclear powers will not have truly survivable forces—seem prone to go up as the number of nuclear powers grows. 80 Moreover, the risk of “unforeseen crisis dynamics” that could spin out of control is also higher as the number of nuclear powers increases. Finally, add to these concerns the enhanced danger of nuclear leakage, and a world with overall higher levels of security competition becomes yet more worrisome. The argument that maintaining Eurasian peace is not a U.S. interest faces a second problem. On widely accepted realist assumptions, acknowledging that U.S. engagement preserves peace dramatically narrows the difference between retrenchment and deep engagement. For many supporters of retrenchment, the optimal strategy for a power such as the United States, which has attained regional hegemony and is separated from other great powers by oceans, is offshore balancing: stay over the horizon and “pass the buck” to local powers to do the dangerous work of counterbalancing any local rising power. The United States should commit to onshore balancing only when local balancing is likely to fail and a great power appears to be a credible contender for regional hegemony, as in the cases of Germany, Japan, and the Soviet Union in the midtwentieth century. The problem is that China’s rise puts the possibility of its attaining regional hegemony on the table, at least in the medium to long term. As Mearsheimer notes, “The United States will have to play a key role in countering China, because its Asian neighbors are not strong enough to do it by themselves.” 81 Therefore, unless China’s rise stalls, “the United States is likely to act toward China similar to the way it behaved toward the Soviet Union during the Cold War.” 82 It follows that the United States should take no action that would compromise its capacity to move to onshore balancing in the future. It will need to maintain key alliance relationships in Asia as well as the formidably expensive military capacity to intervene there. The implication is to get out of Iraq and Afghanistan, reduce the presence in Europe, and pivot to Asia— just what the United States is doing. 83 In sum, the argument that U.S. security commitments are unnecessary for peace is countered by a lot of scholarship, including highly influential realist scholarship. In addition, the argument that Eurasian peace is unnecessary for U.S. security is weakened by the potential for a large number of nasty security consequences as well as the need to retain a latent onshore balancing capacity that dramatically reduces the savings retrenchment might bring. Moreover, switching between offshore and onshore balancing could well be difªcult. Bringing together the thrust of many of the arguments discussed so far underlines the degree to which the case for retrenchment misses the underlyinglogic ofthedeep engagementstrategy. By supplying reassurance, deterrence, and active management, the United States lowers security competition in the world’s key regions, thereby preventing the emergence of a hothouse atmosphere for growing new military capabilities. Alliance ties dissuade partners from ramping up and also provide leverage to prevent military transfers to potential rivals. On top of all this, the United States’ formidable military machine may deter entry by potential rivals. Current great power military expenditures as a percentage of GDP are at historical lows, and thus far other major powers have shied away from seeking to match top-end U.S. military capabilities. In addition, they have so far been careful to avoid attracting the “focused enmity” of the United States. 84 All of the world’s most modern militaries are U.S. allies (America’s alliance system of more than sixty countries now accounts for some 80 percent of global military spending), and the gap between the U.S. military capability and that of potential rivals is by many measures growing rather than shrinking. 85

#### American leadership is sustainable but only if we protect our economy and military

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 hiegth of its power.

#### Second is US-Sino War

#### A lack of international guidelines on cyber warfare makes nuclear escalation by the U.S likely

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.¶

#### Recent tech developments make US cyberdefenses weak and an attack more probable

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

#### China has gained a competitive advantage in Cuba because of U.S. sanctions

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 and push out China

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.

#### Pushing out Chinese companies now is key – shares are falling and they are vulnerable

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.

# Solvency

#### The office of foreign assets control has authority over US sanctions enforcement- by issuing specific licenses, they allow for trade in telecommunications

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.

#### **Past instances of targeted communications licenses prove OFAC has authority**

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.

#### 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

#### 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 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.