# ENCRYPTION CASE NEGATIVE

## A2 INHERENCY

### encryption legal

#### Encryption for IT companies legal -- CALEA

Cindy **Cohn** 10/17/**14--** Cohn is the Executive Director of the Electronic Frontier Foundation and graduate of the University of Michigan Law School. The National Law Journal named Ms. Cohn one of 100 most influential lawyers in America in 2013. Served as the outside lead attorney in Bernstein v. Dept. of Justice, First Amendment challenge to the U.S. export restrictions on cryptography. In 2007 the National Law Journal one of the 50 most influential women lawyers in America. Specializes in NSA surveillance law and serves as council to various surveillance Supreme Court cases. (Cohn, “EFF Response to FBI Director Comey's Speech on Encryption”, Electronic Fronteir Foundation. <https://www.eff.org/deeplinks/2014/10/eff-response-fbi-director-comeys-speech-encryption>)//ET

Here's the relevant part of CALEA that Comey wants to effectively undo: "47 USC 1002(b)(3): A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." Also from the CALEA legislative history: "Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. This obligation is consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4). Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access ... Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, section 2602 protects the right to use encryption." H/T Chris Soghoian: http://paranoia.dubfire.net/2010/09/calea-and-encryption.html

### no backdoors

#### Backdoor installation not happening – 3 reasons

Soghoian et al 15 (Christopher Soghoian, researcher at Harvard and Yale, Kevin Bankston, Policy Director of New America’s Open Technology Institute, Fred Cate, C. Ben Dutton Professor of Law at Indiana University Maurer School of Law, Chris Hoofnagle, Co-Director, Berkeley Center for Law & Technology, Marcia Hofmann, senior staff attorney at the Electronic Frontier Foundation, Rob Faris, Research Director of the Berkman Center for Internet and Society at Harvard University, Albert Gidari, partner of Perkins Coie in Privacy & Security, Jennifer Granick, Director of Civil Liberties for the Center for Internet and Society at Stanford Law School, Orin Kerr, professor of law at the George Washington University , Susan Landau, Professor of Social Science and Policy Studies at Worcester Polytechnic Institute, Paul Ohm, Professor of Law at the Georgetown University Law Center, Nicole Azer, Technology & Civil Liberties Policy Director in ACLU California, John Palfrey, previous executive director of Harvard's Berkman Center for Internet & Society, Marc Rotenberg, President and Executive Director of the Electronic Privacy Information Center, Adam Schostack, expert in security, Ryan Singel, journalist of technology at WIRED, Adam Thierer, senior research fellow with the Technology Policy Program at the Mercatus Center at George Mason University, Jonathan Zittrain, professor of Internet law and the George Bemis Professor of International Law at Harvard Law School, “Privacy And Law Enforcement: Caught In The Cloud: Privacy, Encryption, And Government Back Doors In The Web 2.0 Era”, 12/16/13, <http://www.researchgate.net/publication/228365094_Privacy_And_Law_Enforcement_Caught_In_The_Cloud_Privacy_Encryption_And_Government_Back_Doors_In_The_Web_2.0_Era>, page 417-419)//EM

Traditional Software is Pretty Hard to Covertly Back Door One of the defining features of the Internet era is the ability of technology firms to later fix problems in their products, to release new features after the date of initial sale, and in some cases, to even remove useful features.198 A fix that would in years past have required a costly and slow product recall can now be deployed to all customers with a mere software update. This ability to release products half-finished, rushing them to the market confident in the knowledge that remaining issues can be fixed with a later patch has led to a situation that some experts call a state of perpetual beta.199 In many cases, these updates must be manually downloaded and installed by the user. When this is the case, adoption rates can be extremely low.200 This can lead to problems for government agencies that wish to compel a traditional software company, such as an operating system vendor, into creating and deploying a back door. If users cannot be convinced to download and install critical security updates that might protect them from hackers, how can they be convinced to download and install government back doors that will pilfer their private files. Another problem associated with the insertion of back doors in traditional software products is the fact that most vendors do not know their customers’ identities. Many copies of Microsoft Windows and other software suites are bundled with new computers, negotiated as part of site licenses for companies and universities. Unless the user registers their software installation, the software supplier simply will not know which individual is associated with any particular computer. The widespread problem of software piracy makes this even worse, since these users are even less likely to register their illicit installations under their own names. This inability to tie an identifiable customer to a particular software installation poses a serious barrier to the government’s ability to compel most traditional software providers into rolling out covert back doors, even if the customer can be convinced to install it. Sure, the company can opt to supply to the sneaky update to all customers based on the assumption that the government’s suspect will be one of the impacted users. However, this approach is likely to draw the attention of security researchers and hackers who routinely reverse engineer software updates

#### NSA moving away from back doors now

Joel **Hruska** 4/13/**15—**IT reviewer and journalist for Extreme Tech covering the impacts of policy on IT. (Hruska, “The NSA wants ‘front door’ access to your encrypted data”, Extreme Tech. http://www.extremetech.com/extreme/203275-the-nsa-wants-front-door-access-to-your-encrypted-data)//ET

Last December, I had the opportunity to travel to the Netherlands to meet with multiple European tech companies, web hosts, and other infrastructure providers. The topic of intelligence agency backdoors and US corporate involvement with such policies came up more than once, often in not-entirely-friendly ways. It’s therefore refreshing to see the head of the NSA, Admiral Michael S. Rogers, state up front that the NSA isn’t interested in a backdoor solution to digital surveillance. Instead, he wants a so-called “front-door” solution — which could be even worse. Instead of handing the NSA a unilateral window into encrypted communications taking place at Google or Apple, Rogers suggested a future in which the encryption keys to access such information would be divided between at least two groups — possibly more. In the simplest example, Google would retain half the key, while the NSA held the other half. Thus, the agency wouldn’t be able to unilaterally snoop inside anyone’s files — it would need Google’s support. “I don’t want a back door,” Rogers, the director of the nation’s top electronic spy agency, said during a speech at Princeton University, according to the Washington Post. “I want a front door. And I want the front door to have multiple locks. Big locks.”

### no mandate

#### There’s no backdoor mandate now nor coming

Ackerman 15 (Spencer, national security editor for Guardian US. A former senior writer for Wired, 2012 National Magazine Award for Digital Reporting, “FBI chief wants 'backdoor access' to encrypted communications to fight Isis”, 7/8/15, <http://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis>) WZ

The director of the Federal Bureau of Investigation has warned US senators that the threat from the Islamic State merits a “debate” about limiting commercial encryption – the linchpin of digital security – despite a growing chorus of technical experts who say that undermining encryption would prove an enormous boon for hackers, cybercriminals, foreign spies and terrorists. In a twin pair of appearances before the Senate’s judiciary and intelligence committees on Wednesday, James Comey testified that Isis’s use of end-to-end encryption, whereby the messaging service being used to send information does not have access to the decryption keys of those who receive it, helped the group place a “devil” on the shoulders of potential recruits “saying kill, kill, kill, kill”. Comey said that while the FBI is thus far disrupting Isis plots, “I cannot see me stopping these indefinitely”. He added: “I am not trying to scare folks.” Since October, following Apple’s decision to bolster its mobile-device security, Comey has called for a “debate” about inserting “back doors” – or “front doors”, as he prefers to call them – into encryption software, warning that “encryption threatens to lead us all to a very, very dark place”. But Comey and deputy attorney general Sally Quillian Yates testified that they do not at the moment envision proposing legislation to mandate surreptitious or backdoor access to law enforcement. Both said they did not wish the government to itself hold user encryption keys and preferred to “engage” communications providers for access, though technicians have stated that what Comey and Yates seek is fundamentally incompatible with end-to-end encryption. Comey, who is not a software engineer, said his response to that was: “Really?” He framed himself as an advocate of commercial encryption to protect personal data who believed that the finest minds of Silicon Valley can invent new modes of encryption that can work for US law enforcement and intelligence agencies without inevitably introducing security flaws. While the FBI director did not specifically cite which encrypted messaging apps Isis uses, the Guardian reported in December that its grand mufti used WhatsApp to communicate with his former mentor. WhatsApp adopted end-to-end encryption last year. “I think we need to provide a court-ordered process for obtaining that data,” said Dianne Feinstein, the California Democrat and former intelligence committee chair who represents Silicon Valley. But Comey’s campaign against encryption has run into a wall of opposition from digital security experts and engineers. Their response is that there is no technical way to insert a back door into security systems for governments that does not leave the door ajar for anyone – hackers, criminals, foreign intelligence services – to exploit and gain access to enormous treasure troves of user data, including medical records, financial information and much more. The cybersecurity expert Susan Landau, writing on the prominent blog Lawfare, called Comey’s vision of a security flaw only the US government could exploit “magical thinking”. Comey is aided in his fight against encryption by two allies, one natural and the other accidental. The natural ally is the National Security Agency director, Michael Rogers, who in February sparred with Yahoo’s chief of information security when the Yahoo official likened the anti-crypto push to “drilling a hole in the windshield”, saying: “I just believe that this is achievable. We’ll have to work our way through it.” The Guardian, thanks to Edward Snowden’s disclosures, revealed in September 2013 that the NSA already undermines encryption. The less obvious ally is China, whom the FBI blamed last month for stealing a massive hoard of federal personnel data. In May, China unveiled a national security law calling for “secure and controllable” technologies, something US and foreign companies fear is a prelude to a demand for backdoor entry into companies’ encryption software or outright provision of encryption keys. Without ever mentioning his own FBI director’s and NSA director’s similar demands, Barack Obama castigated China’s anti-encryption push in March. Obama has also declined to criticize efforts in the UK, the US’s premier foreign ally, to undermine encryption. Prime minister David Cameron is proposing to introduce legislation in the autumn to force companies such as Apple, Google and Microsoft to provide access to encrypted data. Under questioning from some skeptical senators, Comey made a number of concessions. When Ron Wyden, an Oregon Democrat, asked if foreign countries would attempt to mandate similar access, Comey replied, “I think they might.” The director acknowledged that foreign companies, exempt from any hypothetical US mandate, would be free to market encryption software. In advance of Comey’s testimony, several of the world’s leading cryptographers, alarmed by the return of a battle they thought won during the 1990s “Crypto Wars”, rejected the effort as pernicious from a security perspective and technologically illiterate. A paper they released on Tuesday, called “Keys Under Doormats”, said the transatlantic effort to insert backdoors into encryption was “unworkable in practice, raise[s] enormous legal and ethical questions, and would undo progress on security at a time when internet vulnerabilities are causing extreme economic harm”. Asked by Feinstein if the experts had a point, Comey said: “Maybe. If that’s the case, I guess we’re stuck.” Kevin Bankston of the New America Foundation called into question the necessity of Comey’s warnings that encryption would lead to law enforcement “going dark” against threats. Bankston, in a Tuesday blogpost, noted that the government’s latest wiretap disclosure found that state and federal governments could not access four encrypted conversations out of 3,554 wiretapped in 2014. Yet Yates said both that the Justice Department was “increasingly” facing the encryption challenge and that she lacked the data quantifying how serious the challenge was. Yates told the Senate judiciary committee that law enforcement declined to seek warrants in cases of encrypted communications and did not say how often it made such a decision.

## A2 SOLVENCY – General

### plan fails

#### Backdoors inevitable – plan fails

#### Lewis 13

James Lewis(James Andrew Lewis is a senior fellow and program director at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes work on Asian politico-military issues, as a negotiator on conventional arms and technology transfers, and on military and intelligence-related technologies. Lewis led the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civil and military technologies and was the rapporteur for the UN Group of Government Experts on Information Security for their successful 2010 and 2013 sessions. He was assigned to U.S. Southern Command for Operation Just Cause, U.S. Central Command for Operation Desert Shield, and to the U.S. Central American Task Force] <http://csis.org/publication/backdoors-and-encryption>) There is a general myth that the “geeks” defeated the Feds in the “crypto wars” of the 1990s, blocking efforts to prevent the sale and export of advanced encryption products. This is an article of faith with some people, particularly on the West Coast, and if you interview them you will get this story presented as an accurate account of what happened. An article in the New York Times hinted at a more accurate picture. The geeks did not win the crypto war. They were deluded into thinking they had done so, producing a false sense of security. Now, wounded that their cherished myth has been punctured like a balloon, they claim that the NSA coerced IT companies to build back doors into encryption products and this is what let it defeat encryption. This is wishful thinking. Wishful because the backdoor argument points to what is one central myth of the internet – that it is possible to use technology to make it secure. If only there weren’t back doors put in by coercion, then we could be safe. Sorry, but while security measures can make it harder to steal data, there are perhaps half a dozen intelligence agencies in the world with the resources and skills to defeat any internet security measure without the need for backdoors. The internet can be made more secure, but it will never be fully secure. The notion of back doors leads immediately to bad policy, and this was the one point that gave me pause in writing this piece. Should I tell them that their proposed fix is useless? If the capabilities that let an intelligence agency defeat encryption do not rely on back doors, switching to foreign products will not make you any safer, although it may provide a degree of comfort rather like an umbrella in a hurricane.

#### SDA is insufficient – fails to close backdoors

Newman 14 (Lily Hay Newman, Future Tense, a partnership of Slate, New America, and Arizona State University, “Senator Proposes Bill to Prohibit Government-Mandated Backdoors in Smartphones,” 12-5-2014, http://www.slate.com/blogs/future\_tense/2014/12/05/senator\_wyden\_proposes\_secure\_data\_act\_to\_keep\_government\_agencies\_from.html)

It's worth noting, though, that the Secure Data Act doesn't actually prohibit backdoors—it just prohibits agencies from mandating them. There are a lot of other types of pressure government groups could still use to influence the creation of backdoors, even if they couldn't flat-out demand them. Here's the wording in the bill: "No agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency."

## A2 ADV – CYBERSECURITY

### sq solves

#### SQUO solves, private companies are already increasing encryption standards

Kharpal 15 – News Assistant for CNBC in London (Arjun, “iPhone encryption 'petrified’ NSA: Greenwald”, 3/18/15, http://www.cnbc.com/2015/03/18/iphone-encryption-petrified-nsa-greenwald.html)

Stronger encryption in Apple's iPhones and on websites like Facebook has "petrified" the U.S. government because it has made it harder to spy on communications, Glenn Greenwald, the writer who first reported on Edward Snowden's stolen files, told CNBC. Former National Security Agency (NSA) contractor Edward Snowden caused major shockwaves around the world in 2013 when he unveiled the surveillance body's wide ranging spying practices, which included regularly attempting to snoop of data held by major technology companies. Glenn Greenwald, the man who helped Snowden publish the documents, said that Silicon Valley companies have bolstered the encryption on their products, thereby making it harder for governments to eavesdrop. "They (Apple) are now starting to put serious encryption technologies in their new iPhones in their new releases and this has really petrified governments around the world," Greenwald told CNBC in an interview at tech fair CeBIT in Germany. Apple, Google, Facebook and Yahoo are some of the major companies that have been in the spotlight after Snowden's revelations. Information from the Snowden documents released earlier this month detailed how the CIA had been trying for a decade to crack the security in Apple's products. And last year, Yahoo revealed that it was threatened with a $250,000 per day fine if it didn't hand over data to the NSA. The tech giants have been taking major steps to make sure their communications are safe from spying, a move Greenwald – who won a Pulitzer prize for his reporting on the topic – said was motivated by the fear of losing customers rather than care for data privacy. "I don't…(think) they suddenly care about privacy," Greenwald said. "If…you're a Facebook executive or an Apple executive, you're extremely worried that the next generation of users…are going to be vulnerable to the pitch from Brazilian, and Korean and German social media companies where they advertise and say don't use Facebook and Google because they'll give your data to the NSA." Snowden is due to address CeBIT later today.

### investigations turn

#### They’ve got it backwards – vulnerabilities are inevitable and backdoors are key to cybersecurity

Hess, Executive Assistant Director of the FBI, 15 (Amy Hess, Executive Assistant Director of the FBI, “ENCRYPTION TECHNOLOGY POLICY ISSUES”, 4/29/15, HTTP://congressional.proquest.com.proxy.lib.umich.edu/congressional/docview/t39.d40.04293003.d94?accountid=14667)//EM

The reality is that cyber adversaries will exploit any vulnerability they find. But security risks are better addressed by developing solutions during the design phase of a specific product or service, rather than resorting to a patchwork solution when law enforcement presents the company with a court order after the product or service has been deployed. To be clear, we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data. We have been on the front lines of the fight against cybercrime and economic espionage and we recognize that absolute security does not exist in either the physical or digital world. Any lawful intercept or access solution should not lower the overall security. But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets.

### tracking turn

#### Turn – encrypted software doesn’t allow for malware tracking, increasing the amount of successful hacks

Aggarwal 15 (Varun, Principal Correspondent at The Economic Times, “Here's how data encryption is making companies less secure”, 14 April 2015, http://articles.economictimes.indiatimes.com/2015-04-14/news/61142361\_1\_malware-credit-card-data-theft-encryption)

While security experts have been advising companies to encrypt all their sensitive data to secure themselves post the NSA snooping scandal, a new study by Dell reveals that encryption could be doing just the opposite. "Although there are many benefits to using more Internet encryption, we are seeing a less positive trend emerge as hackers exploit this encryption as a way of "hiding" malware from corporate firewalls," Amit Singh, country manager, Dell SonicWALL, India, told ET. In early 2014, hackers successfully distributed malware to about 27,000 Europeans per hour over the course of four days, simply by infecting a group of banner advertisements on Yahoo's news site. "Since Yahoo's site was encrypted, this malware was able to tunnel through users' firewalls unseen," Dell's annual security threat report said. Dell saw an increase in the volume of HTTPS web connections from 182 billion in January 2014 to 382 billion in January 2015, and this number continues to grow. As of March 2015, the number was 437 billion. "More companies were exposed to attackers hiding in plain sight as a result of SSL/TLS encrypted traffic. For many years, financial institutions and other companies that deal with sensitive information have opted for the secure HTTPS protocol that encrypts information being shared. Now other sites like Google, Facebook, and Twitter are adopting this practice as well in response to a growing demand for user privacy and security," the report said. "The only way to manage this threat is by using new age firewalls that provide SSL inspection, thereby telling you if there is any malicious code in the encrypted traffic," Singh said. The report also highlighted a spike in attacks on retail point of sale systems. In US, Home Depot, Target, Michaels, and Staples all became targets of credit card data theft, with each breach exposing millions of consumers to potential fraudulent purchases and/or identity theft. Target's was considered the largest breach in the history of U.S. retail, with 40 million card numbers stolen, until Home Depot's breach compromised 56 million card numbers just a few months later. In the case of Home Depot and Michaels, the attacks took place over several months before they were detected. Dell SonicWALL saw 13 new types of POS malware in 2014, compared with three in 2013 - a 333% increase in the number of new POS malware countermeasures developed and deployed. The majority of these POS hits targeted the U.S. retail industry. However, Singh said with the growth of retail in India, Indian customers could possibly face similar attacks

### no attacks

#### Cyberwar isn’t happening, hasn’t happened, and won’t happen

Rid 2013 (Thomas Rid reader in the department of war studies at King’s College London and the author of “Cyber War Will Not Take Place”, New Scientist issue 2933 “Why a Cyberwar Won’t Happen 07/07/2013 https://www.newscientist.com/article/mg21929334.800-why-a-cyberwar-wont-happen/)NF

Leaks revealed last week that the US government spends a staggering $4.3 billion a year on cyber operations. In 2011, American intelligence agencies reportedly mounted [231 offensive operations](http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?wpisrc=nl_cuzheads). The US, it seems, is gearing up for cyber combat. What would an act of cyberwar look like? History suggests three features. To count as an armed attack, a computer breach would need to be violent. If it can’t hurt or kill, it can’t be war. An act of cyberwar would also need to be instrumental. In a military confrontation, one party generally uses force to compel the other party to do something they would otherwise not do. Finally, it would need to be political, in the sense that one opponent says, “If you don’t do X, we’ll strike you.” That’s the gist of two centuries of strategic thought. No past cyberattack meets these criteria. Very few meet even a single one. Never has a human been injured or hurt as an immediate consequence of a cyberattack. Never did a state coerce another state by cyberattack. Very rarely did state-sponsored offenders take credit for an attack. So if we’re talking about war – the real thing, not a metaphor, as in the “war on drugs” – then cyberwar has never happened in the past, is not taking place at present, and seems unlikely in the future. “Cyberwar has not taken place in the past, is not taking place at present and is unlikely in the future” That is not to say that cyberattacks do not happen. In 2010, the US and Israel attacked Iran’s nuclear enrichment programme with a computer worm called Stuxnet. A computer breach could cause an electricity blackout or interrupt a city’s water supply, although that also has never happened. If that isn’t war, what is it? Such attacks are better understood as either sabotage, espionage or subversion. Code-borne sabotage is a real risk. Industrial control systems run all sorts of things that move fast and can burn: trains, gas pipelines, civilian aircraft, refineries, even elevators and medical devices. Many of these are highly susceptible to breaches, and information about system vulnerabilities is easily available. Even so, the number of violent computer-sabotage attacks against Western targets is zero. Why? Because causing havoc through weaponised code is harder than it looks. Target intelligence is needed. Control systems are often configured for specific tasks, limiting the possibility of generic attacks. Even if they happened, such attacks may not constitute a use of force. The second threat is cyber espionage. Data breaches are not just a risk, but a real bleeding wound for the US, Europe and other advanced economies. But espionage is not war, and cyber espionage is not cyberwar. Finally, there is subversion – using social media and other internet services to undermine established authority. It is not a surprise that subversives, from Anonymous and Occupy to Arab protesters, use new technologies. Twitter and Facebook have made organising non-violent protest easier than ever, often in the service of liberty and freedom. But again, subversion is not war, and cyber subversion is not cyberwar. There are other problems with the concept of cyberwar. First, it is misleading. Closer examination of the facts reveals that what is happening is the opposite of war: computer breaches are less violent than old-style attacks. Violent sabotage is harder if it is done through computers, while non-violent sabotage is now easier and is happening more often: crashing websites, deleting files and so on. The same goes for espionage: infiltrating software and opening remote back doors is much less risky than sending in human agents and clandestinely bugging embassy walls.

#### Cyberattacks aren’t enough for terrorists- they don’t care

Lewis 02 (James A. Lewis, Director and Senior Fellow of the technology and public policy program at the center for strategic and international studies at Washington, D.C., Former member of U.S. Foreign Service and Senior Executive Service, Ph.D. from University of Chicago, Center for Strategic and International Studies “Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats” December 202 page 9-10 http://www.steptoe.com/publications/231a.pdf)NF

Much of the early work on the ‘cyber threat’ depicted hackers, terrorists, foreign spies and criminal gangs who, by typing a few commands into a computer, can take over or disrupt the critical infrastructure of entire nations. This frightening scenario is not supported by any evidence. Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations. Cyber-terrorism has attracted considerable attention, but to date, it has meant little more than propaganda, intelligence collection or the digital equivalent of graffiti, with groups defacing each other’s websites. No critical infrastructures have been shut down by cyber attacks. Terrorists seek to make a political statement and to inflict psychological and physical damage on their targets. If terrorism is an act of violence to achieve political objects, how useful will terrorists find an economic weapon whose effects are gradual and cumulative? One of Al Qaeda’s training manuals, “Military Studies in the Jihad Against the Tyrants” notes that explosives are the preferred weapon of terrorist because “explosives strike the enemy with sheer terror and fright.” Explosions are dramatic, strike fear into the hearts of opponents and do lasting damage. Cyber attacks would not have the same dramatic and political effect that terrorists seek. A cyber attack, which might not even be noticed by its victims, or attributed to routine delays or outages, will not be their preferred weapon. If terrorism is an act of violence to create shock and achieve political objects, how useful will terrorists find an economic tool whose effects are at best gradual and cumulative?

## A2 ADV – ECON

### sq solves econ

#### Status quo solves – USA economy high right now

Mutikani 7/16 (Lucia, Journalist and Correspondent for Thomson Reuters, “U.S. jobless claims, housing data point to firming economy”, http://www.reuters.com/article/2015/07/16/us-usa-economy-jobs-idUSKCN0PQ1AJ20150716)

The number of Americans filing new applications for unemployment benefits fell more than expected last week and confidence among homebuilders held at a more than 9-1/2-year high in July, indicating underlying momentum in the economy. The solid labor market and firming housing sector, underscored by Thursday's reports, suggest the economy likely is strong enough to support an interest rate hike this year. Manufacturing, however, continues to struggle. "Overall, the economy continues to move in the right direction. We look for the Federal Reserve to hike rates twice before the end of the year beginning in September," said John Ryding, chief economist at RDQ Economics in New York.Fed Chair Janet Yellen told lawmakers on Wednesday that the U.S. central bank remained on course to tighten monetary policy "at some point this year." Initial claims for state unemployment benefits fell 15,000 to a seasonally adjusted 281,000 for the week ended July 11, the Labor Department reported. The decline reversed the prior week's rise and ended three straight weeks of increases. Economists had forecast claims falling to 285,000 last week. While claims tend to be volatile during the summer when automakers normally shut assembly plants for annual retooling, a Labor Department official said there was nothing unusual in the state-level data. Some automakers keep production running, which can throw off a model the government uses to smooth the data for seasonal fluctuations. The four-week moving average of claims, considered a better measure of labor market trends as it irons out week-to-week volatility, increased 3,250 to 282,500 last week. It was the 16th straight week that the four-week moving average of claims held below 300,000, a threshold normally associated with a firming labor market. The dollar rose against a basket of currencies, while prices for short-dated U.S. government debt fell. Stocks on Wall Street were higher after Greece's Parliament voted to approve a new bailout program and Citigroup (C.N) reported its highest quarterly profit in eight years

### no econ impact

#### No chance of war from economic decline---best and most recent data

Drezner 12 [Daniel W., Professor, The Fletcher School of Law and Diplomacy, Tufts University, “The Irony of Global Economic Governance: The System Worked,” International Institutions and Global Governance Program, October 2012, <http://www.cfr.org/international-organizations-and-alliances/irony-global-economic-governance-system-worked/p29101>, July 17, 2015] KL

The final outcome addresses a dog that hasn’t barked: the effect of the Great Recession on cross-border conflict and violence. During the initial stages of the crisis, multiple analysts asserted that the financial crisis would lead states to increase their use of force as a tool for staying in power.37 Whether through greater internal repression, diversionary wars, arms races, or a ratcheting up of great power conflict, there were genuine concerns that the global economic downturn would lead to an increase in conflict. Violence in the Middle East, border disputes in the South China Sea, and even the disruptions of the Occupy movement fuel impressions of surge in global public disorder. The aggregate data suggests otherwise, however. The Institute for Economics and Peace has constructed a “Global Peace Index” annually since 2007. A key conclusion they draw from the 2012 report is that “The average level of peacefulness in 2012 is approximately the same as it was in 2007.”38 Interstate violence in particular has declined since the start of the financial crisis – as have military expenditures in most sampled countries. Other studies confirm that the Great Recession has not triggered any increase in violent conflict; the secular decline in violence that started with the end of the Cold War has not been reversed.39 Rogers Brubaker concludes, “the crisis has not to date generated the surge in protectionist nationalism or ethnic exclusion that might have been expected.”40 None of these data suggest that the global economy is operating swimmingly. Growth remains unbalanced and fragile, and has clearly slowed in 2012. Transnational capital flows remain depressed compared to pre-crisis levels, primarily due to a drying up of cross-border interbank lending in Europe. Currency volatility remains an ongoing concern. Compared to the aftermath of other postwar recessions, growth in output, investment, and employment in the developed world have all lagged behind. But the Great Recession is not like other postwar recessions in either scope or kind; expecting a standard “V”-shaped recovery was unreasonable. One financial analyst characterized the post-2008 global economy as in a state of “contained depression.”41 The key word is “contained,” however. Given the severity, reach and depth of the 2008 financial crisis, the proper comparison is with Great Depression. And by that standard, the outcome variables look impressive. As Carmen Reinhart and Kenneth Rogoff concluded in This Time is Different: “that its macroeconomic outcome has been only the most severe global recession since World War II – and not even worse – must be regarded as fortunate.”42

#### Economic doesn’t doesn’t lead to conflict

Zakaria 09 (Fareed, was the managing editor of Foreign Affairs, Ph.D. in political science from Harvard, “The Secrets of Stability”, Newsweek, 12/11/09, http://www.thedailybeast.com/newsweek/2009/12/11/the-secrets-of-stability.html)

Others predicted that these economic shocks would lead to political instability and violence in the worst-hit countries. At his confirmation hearing in February, the new U.S. director of national intelligence, Adm. Dennis Blair, cautioned the Senate that "the financial crisis and global recession are likely to produce a wave of economic crises in emerging-market nations over the next year." Hillary Clinton endorsed this grim view. And she was hardly alone. Foreign Policy ran a cover story predicting serious unrest in several emerging markets. Of one thing everyone was sure: nothing would ever be the same again. Not the financial industry, not capitalism, not globalization. One year later, how much has the world really changed? Well, Wall Street is home to two fewer investment banks (three, if you count Merrill Lynch). Some regional banks have gone bust. There was some turmoil in Moldova and (entirely unrelated to the financial crisis) in Iran. Severe problems remain, like high unemployment in the West, and we face new problems caused by responses to the crisis—soaring debt and fears of inflation. But overall, things look nothing like they did in the 1930s. The predictions of economic and political collapse have not materialized at all. A key measure of fear and fragility is the ability of poor and unstable countries to borrow money on the debt markets. So consider this: the sovereign bonds of tottering Pakistan have returned 168 percent so far this year. All this doesn't add up to a recovery yet, but it does reflect a return to some level of normalcy. And that rebound has been so rapid that even the shrewdest observers remain puzzled. "The question I have at the back of my head is 'Is that it?' " says Charles Kaye, the co-head of Warburg Pincus. "We had this huge crisis, and now we're back to business as usual?"

### investment turn

#### Fear of surveillance is driving encryption investment – funding increasing now

JIJI 14 <Press news journal covering business and economics, 3/29/14, “The ‘golden age’ of encryption?”, The Japan Times, http://www.japantimes.co.jp/news/2014/03/29/business/tech/the-golden-age-of-encryption/#.VamBOMZVikp>//wx

NEW YORK – Investors are pumping millions of dollars into encryption as unease about data security drives a rising need for ways to keep unwanted eyes away from personal and corporate information. Major data breaches at Target and other retailers have made data security a boardroom issue at companies large and small. And stunning revelations of widespread snooping by U.S. intelligence agencies have also rattled companies and the public. For venture capital, that has opened up a new area of growth in the tech business. In February, Google Ventures led a $25.5 million round of venture funding for Atlanta-based Ionic Security, a 3-year-old company that works on encryption — the scrambling of data before it is shipped or stored. Other encryption companies, including Toronto-based PerspecSys and San Jose, California-based CipherCloud, have announced major fundings. The funding rush could hearken a “golden age” of encryption, as one expert puts it. But the industry also faces barriers to a tool that until recently was not a hot commodity. Concerns about encryption range from practical challenges, such as the difficulty people have when searching for something in their encoded data, to government opposition toward privacy technology. “People are afraid of it because they don’t understand it,” said John Kindervag, a vice president and principal analyst at Forrester Research. But he called the wider use of encryption “inevitable, because there’s no other way to solve the problem.” Kindervag said the industry is between one and two years away from “some big revolutions” in the field. “It just needs to happen,” he added. But Venky Ganesan, a managing director with venture capital firm Menlo Ventures, believes major advances are further off. “Encryption slows down,” Ganesan said. “Just imagine if every room in your house was locked and you had to open and close it every time you go in. You would be frustrated.”

#### Lack of incentive for investment kills startups – liquidated too quickly

Primack 15 <Dan, senior editor at Fortune, cites top VC and investor Bill Gurley, 1/22/15, “Top VC: A lot of tech startup failure coming in 2015”, http://fortune.com/2015/01/22/vc-tech-startup-failure-2015/>//wx

Bill Gurley thinks that some highly-valued tech startups are heading for a reckoning. Bill Gurley is no stranger to unicorns, the tech industry’s name for startups that have been valued at $1 billion or more by venture capitalists. His VC firm, Benchmark, has put money into such companies as Uber, DropBox, SnapChat and WeWork. Not to mention some that recently went public, like Hortonworks and New Relic . But he believes that many of these unicorns, of which there are more than 80, will go down in flames after flying too close to the sun. “I think you’re going to see a lot of failure in 2015,” Gurley said in Fortune‘s [February cover story](http://fortune.com/2015/01/22/the-age-of-unicorns) on the unicorn trend. Some companies will collapse under their own overvalued weight, others because there could be a macro financial pullback that filters down into the private markets. Here is Gurley’s primary concern: Privately-held companies that raise lots of funding at higher and higher valuations eventually build up tons of liquidation preferences. For the jargon-challenged, liquidation preferences are inserted into venture funding deals to ensure that the VC gets paid first (and how much) if the company is sold (i.e., generates liquidity). If a company is sold at a massive valuation increase, then it’s largely academic, as everyone gets rich. But if the company is sold at a price below where it last raised money, it could leave a bunch of people out in the cold, including employees who were largely compensated with stock options. “The cap chart begins to calcify a bit, which eventually can be problematic,” Gurley explains. “Hiring new employees, particularly senior management, becomes tough because they worry about getting stuck beneath a huge liquidation preference stack. Some of these deals have so many [anti-dilution terms] that the cap table becomes almost concrete. If the valuation goes down significantly, it will sink them.” This is, of course, different than what happens when a publicly-traded company suffers a major valuation hit. In those cases, the company can still offer stock options to employees at “market” prices, without liquidation preferences getting in the way. Moreover, far too few of these startups are actually profitable, meaning that they are virtually required to keep tacking on new liquidation preferences in subsequent funding rounds. Part of this is because so many entrepreneurs have taken their cue from unprofitable tech giants like Amazon and Salesforce , but the truth is that not everyone is Jeff Bezos or Marc Benioff. “All of these companies raising so much money at higher and higher valuations is becoming a burgeoning anchor,” Gurley says. “I think it’s almost tautologically easier to execute a company that loses money than one that’s profitable.”

## A2 ADV – HUMINT

### sq solves

#### HUMINT funding and recruitment are increasing

#### Henely Putnam University 11

Henley-Putnam University( is the only accredited university that specializes exclusively in intelligence, counterterrorism and protection and offers over 100 courses on topics such as covert actions, counterterrorism and intelligence team management. By completing a degree here you will further differentiate yourself as a specialist among your peers. Pursue a Bachelors or Masters Degree within your chosen specialty , or a Doctorate Degree in Strategic Security. http://www.henleyputnam.edu/intelligencedegrees/humanintelligence.aspx)

Since the terrorist attacks on September 11, 2001, there has been renewed focus on the important role that HUMINT plays in collecting information on terrorist networks and other hostile non-state actors. Consequently, calls for building up a new, robust cadre of HUMINT professionals has led to increase investment in funding and recruiting efforts, especially for foreign language specialists and those who have traveled extensively overseas. At Henley-Putnam University, we offer a nationally accredited [(DETC)](http://www.detc.org/%22%20%5Ct%20%22_blank%22%20%5Co%20%22DETC) program that focuses exclusively on intelligence through our Bachelor and Master of Science Degrees in Intelligence Management. Our 100% online courses are taught by expert faculty with real world experience from the government and intelligence community. Graduates of our highly-focused program will be able to: Manage a team of intelligence professionals from different disciplines, conduct operations that include clandestine or covert activities and present finished intelligence in a manner appropriate to the consumer, to name but a few. Classes cover topics like Advanced Intelligence Operations, Counterespionage, and Intelligence Team Management. Embark on an exciting education path with Henley-Putnam by calling us today

### humint fails

#### HUMINT fails: can’t gather on terrorist groups and new groups pop up

Best, 2 (Richard A. Best Jr., Specialist in National Defense Foreign Affairs, Defense, and Trade Division, CRS report for congress, Wrote *The National Intelligence Council: Issues and Options for Congress* and published in Library of Congress. Pages 9-11 February 21, 2002.)\\mwang

Terrorists do not usually appear on the diplomatic cocktail circuit nor in gatherings of local businessmen. In many cases they are also involved in various types of criminal activities on the margins of society. Terrorist groups may be composed almost wholly of members of one ethnic or religious group. They may routinely engage in criminal activities or human rights abuses. Developing contacts with such groups is obviously a difficult challenge for U.S. intelligence agencies; it requires long-lead time preparation and a willingness to do business with unsavory individuals. It cannot in many cases be undertaken by intelligence agents serving under official cover as diplomats or military attaches. It may require an in-depth knowledge of local dialects and customs. Furthermore, the list of groups around the world that might at some point in the future be involved in terrorist activities is not short; making determinations of where to seek agents whose reporting will only be important under future eventualitiesis a difficult challenge with the risk of needlessly involving the U.S. with corrupt and ruthless individuals. Critics of the current U.S. humint collection effort point to these and other institutional problems. One report quotes a former CIA official: **The CIA probably doesn’t have a single** truly qualified Arabic-speaking officer of Middle Eastern background who can play a believable Muslim fundamentalist who would volunteer to spend years of his life ... in the mountains of Afghanistan need is for greater numbers of foreign language-capable intelligence personnel, with increased fluency in specific and multiple languages. The Committee has heard repeatedly from both military and civilian intelligence producers and consumers that this is the **single greatest limitation in intelligence agency** personnel expertise and that it is a deficiency throughout the Intelligence Community.”

It is administratively difficult to develop resources throughout the world over a long period of time and costs are higher than adding intelligence staff to embassies. Few observers could have predicted the intense U.S. concern with Somalia, Kosovo, or Afghanistan that eventually developed. Ten years from now there may be a whole set of challenges from groups that no one today is even aware of. In short, reorienting humint collection to give significantly greater attention to terrorist or potentially terrorist groups would have important administrative implications for the Intelligence Community. While budgetary increases would not necessarily be dramatic given the size of the existing intelligence budget (even paying hundreds of human agents would be far less costly than deploying a satellite), the infrastructure needed to train and support numerous agents serving under non-official cover would grow significantly. Extensive redundancy would be required to cover terrorist groups that may never pose significant threats to U.S. interests.

#### HUMINT is not key to intelligence gathering – other methods fill in

Sundaraj-Keun 12 (Simon S. Sundaraj-Keun. Think Tank Consultancy (Freelance), Sole-Proprietor Research, Malaysian Dutch Descendents Project (MDDP) formerly at Dalat International School, HarvardX, Specialize background in providing risk assessment Human Resources & Relations expert with wide proficiency in researching, analyzing, and amending organizational frameworks.) "Human Intelligence: Past, Present, and Future”. <<https://simonsundarajkeun.wordpress.com/2012/11/22/human-intelligence-past-present-and-future/>> November 22, 2012.) \\mwang

There are methods of obtaining intelligence like Open Source Intelligence (OSINT) which is the gathering of information from open sources. Signals Intelligence (SIGINT) and Communications Intelligence (COMINT) is the gathering of sources from interception of signals, and Electronic Intelligence (ELINT) is the gathering of Intel from non-communications electronic emissions. For the most part the methods used in obtaining intelligence does not place the human component in a high risk situation. The risks of losing an operative is as real as it can be because the targeted nation can deport, imprison, or even execute a spy. Some nations will deploy counter agents in order to roll up several clandestine networks and even hire agents to infiltrate into other nation’s agency. Sometimes it is not easy to imprison a spy because he or she is given diplomatic immunity by the home nation. The targeted nation can declare persona non grata in order to evict the spy from its borders. It takes a long time to train a HUMINT agent than it takes to replace a broke computer or replace a spy satellite. For cost effectiveness and risk free the United States has placed its emphasis on the development of technologies in order to have command and control in the field of communication. One has to understand that the advancement of technology brought the means and methods of espionage to a new level. The days of agents running around a nation-state has evolved to an era of surveillance of all electronic transmissions including cell phone logs, voice mail, email, packet sniffing, trace routing and wireless transmissions. In reality the prioritization of most intelligence agencies today has been to control and monitor financial transactions, the information corridor (internet and communication lines), and the spread of technological advance weaponry (weapons of mass destruction). In the post-Cold War world numerous agencies have been data mining the world’s stock exchanges and this program was formalized on October 26, 2001 in the form of the Patriot Act. This helps track the financing of people who might be laundering money and continues to be done without any warrants. It is important for any nation to gather the political and economic information that might be of advantage to its Strategic Intelligence. The United States is no exception to the rule and monitoring of foreign communications is essential in maintaining its national interest. In 2002, new programs of satellite surveillance and unmanned low level drones armed with missiles made it possible not only to perform surveillance in real time, but to respond with force. Thus proving that unmanned drones could be used for elimination operations without the lost of Allied forces. One has to understand that out of the advancement of technology, chronic problems begin to emerge in the shadows, which would in turn create an intelligence blind spot that would leave a state’s national security in the dark. This blind spot is the lack of balance between the use of HUMINT and technology as a symbiosis component in force multiplication. The lack of investment in HUMINT could lead to disaster as experience during World War II and currently on the War on Terrorism demonstrates. There is a serious problem faced by HUMINT, which is the lack of time and effort to learn the multiple languages that are spoken by the various ethnic groups within the nations around the globe. Languages transcend beyond the physical boundaries of nation-states and reflect the unique multiracial heritage of a nation. There a firm belief that appreciation of languages should take priority in order to address the intelligence problem, it will help to promote one’s national security, which is unfortunately lacking in today’s global arena (especially in the United States Intelligence community).

### crime turn

#### Crime rates will escalate without encryption backdoors – criminals use encryption

**Tucker and Gillum 14** – Tucker: Covers Justice Department for Associated Press. Gillum: Reporter at the Associated Press. Been at USA TODAY. Columbia University – Graduate School of Journalism. BSc Santa Clara University – Political Science. (“FBI: cellphone encryption would impede criminal investigations”, Eric Tucker and Jack Gillum, Associated Press – Public Broadcast Station, October 16, 2014, http://www.pbs.org/newshour/rundown/fbi-cellphone-encryption-impede-criminal-investigations/)//chiragjain

WASHINGTON — FBI Director James Comey warned in stark terms Thursday against the push by technology companies to encrypt smartphone data and operating systems, arguing that murder cases could be stalled, suspects could walk free and justice could be thwarted by a locked phone or an encrypted hard drive. Privacy advocates and technology experts called the concerns exaggerated and little more than recycled arguments the government has raised against encryption since the early 1990s. Likening encrypted data to a safe that cannot be cracked or a closet door that won’t open, Comey said the move by tech companies to protect user communications in the name of privacy is certain to impede a wide range of criminal investigations. New legislation to allow law enforcement to intercept communications is needed at a time of advancing technology and new forms of communication, he said. “We have the legal authority to intercept and access communications from information pursuant to court order, but we often lack the technical ability to do so,” Comey said in a Brookings Institution speech. Comey cited particular cases in which he said access to cell phone data aided in a criminal investigation. But in a question-and-answer session after the speech, he said he could not cite particular instances in which someone was rescued from danger who wouldn’t have been had law enforcement been blocked from that information. “Logic tells me there are going to be cases like that,” Comey said. The speech, which echoes concerns he and others in law enforcement have previously made, comes soon after announcements by Apple and Google that their new operating systems will be encrypted, or protected with coding by default. Law enforcement officials could still intercept conversations but might not be able to ac cess call data, contacts, photos and email stored on the phone. While the companies’ actions are understandable, Comey said, “the place they are leading us is one we shouldn’t go to without careful thought and debate.” “Encryption isn’t just a technical feature. It’s a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at every level,” Comey said. The government’s concerns may also center in part on the use of Apple’s iMessage platform, which offers end-to-end encrypted text messages that supersede traditional SMS messages. That kind of encryption likely provides access to those messages on users’ iPhones, of which Apple has sold more than 240 million since 2013. He acknowledged a rise in public mistrust of government in the year since former National Security Agency systems analyst revealed NSA secret intelligence collection programs. But he said the public was wrong to believe that law enforcement can access any and all communications with the flip of a switch. “It may be true in the movies or on TV. It is simply not the case in real life,” he said. Comey also said the FBI was committed to a “front-door” approach, through court orders and under strict oversight, to intercepting communications. Privacy advocates have long been concerned that that intercept would create an opening for hackers to exploit. The American Civil Liberties Union said federal law protects the right of companies to add encryption with no backdoors and that the companies should be credited for being “unwilling to weaken security for everyone.” “Whether you call it a ‘front door’ or a ‘back door,’ weakening the security of a system to enable law enforcement access also opens that door to foreign governments and criminals,” said Christopher Soghoian, principal technologist with the ACLU’s Speech, Privacy and Technology Project. Matthew Green, a cryptology professor at Johns Hopkins University, said the debate over personal encryption isn’t new: Back in the 1990s, when personal computers were a novelty, he said most consumers weren’t even aware of encryption. When a form of email encryption called PGP was released, he said, there was a fear that criminals would use it. “These technologies exist” for consumers to protect their privacy, he said, “and it’s very hard to do anything about it.”

#### Encryption is used in many different types of transnational organized crime

**Denning, Wack, Kerins 00** – Denning: American Security Researcher, University of Michigan, Jay Wack – CEO of TecSec, Electronics Career at US Army, Jim Kerins : Information Technology and Security specialist: (“Transnational Crime, Corruption, and Information Technology”, Dorothy Denning, Jay Wack, Jim Kerins, November 30-December 1, 2000, Transnational Crime and Corruption Center, [http://traccc.gmu.edu/pdfs/publications/transnational\_crime\_publications/variou01.pdf)//chiragjain](http://traccc.gmu.edu/pdfs/publications/transnational_crime_publications/variou01.pdf%29//chiragjain)

The third panel focused on the critical interactions among transnational crime, corruption, and information technology. Encryption is often held out as the key advantage that criminals have over law enforcement. Law enforcement and the intelligence community are seeking to limit the strength of encryption keys, noting that encryption slows their investigation and could become unbreakable, thus allowing criminals and others to communication without fear of law enforcement listening in. Privacy advocates, on the other hand, support the need to ensure 14 private, legitimate communications and thus argue against limiting the strength of encryption technologies or providing law enforcement with keys that would allow them access to encrypted communications. The panelists, therefore, examined the merits of these arguments in the context of transnational crime and corruption. The first speaker, Dr. Dorothy Denning, addressed how national organized criminals use encryption and associated technologies. Encryption, according Dr. Denning, is being used in many different contexts, various forms of communications, as well as in the storage of data. The evidence for the use and effects of encryption are currently anecdotal. New guidelines on reporting the results from wiretaps and the instances where encryption frustrates those wiretaps offer some hope for better data in the future. Turning to criminal activities, encryption is used in many different types of crimes, ranging from terrorism to narcotics trafficking and other forms of organized crime. One illustration involved a university professor who allegedly engaged in child pornography and the campus police could not do anything with the files on his computer due to strong encryption. Thus, how does one approach cases that involve encryption? Breaking the method of cryptography or getting the key solves many such cases. Since a password often protects the encryption key itself, investigations often focus on acquiring the password and, in turn, the key to decoding the encryption. In many cases, the cryptography is broken not because the algorithms weren’t of sufficient quality or the keys weren’t long enough, but due to the overall weakness of products and the ability of “brute force” techniques to overcome the encryption— particularly true of most commercial software products until recently. But encryption is not the only issue in this context. Steganography, for example, is related to and yet different from encryption in that encryption is extremely recognizable—one can recognize an encrypted file when one sees it. With steganography, one can hide files not only in images, but also in sound files, video, text, or even in unused space in a disk. Thus, you can use encryption with steganography for added protection and deception. Another issue is anonymity, where all kinds of services and tools exist to provide anonymous communications. Anonymous remailers, for instance, work with electronic mail to shield the source of electronic communications. Finally, the use of hacker tools, especially those designed to cover the tracks of email and to intercept passwords of user accounts, is a topic that one must consider when examining the use of encryption for illicit gains. The next speaker, Jay Wack, sought to provide the private sector’s point of view in the debate between privacy advocates and law enforcement in the encryption field. Focusing on the positive uses for encryption and the fact that privacy components require addressing, it is useful to liken the debate to a scale. On one side is law enforcement, which that would like to know what’s going on all the time. On the other side is the individual, who would like to be able to be anonymous all the time. While this exaggerates the positions of the two sides to illustrate the contrast better, it is important to ask how does one craft an equitable and manageable solution that bridges the gap between the two sides? In order to answer that question, one needs to start with some of the issues that form the engines driving the debate. For one there is issue of privacy itself, or “the right to be left alone.” While simplistic, this statement merely reflects that privacy is a huge problem to contend with in this debate—especially in the US. The continued growth of the Internet and, especially, the connections between massive computerized information systems have led some industry captains to note that era of privacy is over. Hence, when we speak of e-commerce, one of the driving influences behind the collection of information, we must speak of security (i.e. the control and safety of information), confidentiality (i.e. the restriction of access to information), and privacy, or what an information collector does with the database after its creation. 15 Many dynamics of American Internet usage are changing affecting the debate. One is that the US no longer serves as the location for the preeminent groups of the Internet. Although the United States does have in excess of 100 million people using the Internet, this number does not represent the majority of Internet users any longer. Thus, we now must concern ourselves with the fact that we share the Internet with many nationalities simultaneously, and their policies on encryption will impact the debate we are outlining today. The US has laws pushing and/or forcing us into the electronic environment. For example, Medicaid is a paper-based system that takes 65 days to process, and thus we would like to move to an electronic mechanism that takes moments to process. An inherent element of the paper process is its privacy, with it the fact that the paper is folded up, put in an envelope, moved through the mail system. It is confidential in that the envelope prevents others from seeing the contents; and many laws protect the privacy of people’s mail. The problem in moving to an electronic schema is that the medical community now has to provide a similar state of confidentiality as the envelope. Compounding this challenge is to ensure privacy in such a way that the information moves across the network and to make sure that a signature is applied in such a way that the person’s actual identity is confirmed. Thus, a conclusion drawn from the engines described above is that one has to have the means of protecting his or her information on the information highway. From the business side, then, the encryption industry is trying to develop strong software packages that protect digital information while at the same time maintaining the speed that is drawing more information to the Internet. In order to accomplish this, one has to have a secure platform and a secure authentication. It starts with who am I? For example, Bruce Snyder recently wrote an article on the issue of the electronic signature law passed in January 2000. Citing defects in the system, one of the solutions he suggested to strengthen security systems was that they should have a hardware device, and information should not be put on a drive in “soft” form that could lead to theft and abuse. Another solution to ensure privacy is that smart cards be used to harmonize information systems and hardware. In the end, there are solutions available that accommodate the conflicting personal, organizational, and law enforcement interests with regard to encryption. Confidentiality should be under the control of the individual. The concluding speaker on the panel, Jim Kerins, sought to outline the effects, positive and negative, of regulating the production and use of encryption tools and began by reminding the audience of some of the more relevant statistics from earlier in the day. First, that the US is no longer the dominant population on the Internet in terms of access or e-commerce. Next, regardless of whether commerce is business-to-business, business to consumer or consumer to government, there is a virtual environment that provides anonymity in commercial dealings that fraudsters have taken full advantage of. Thus, analysis of fraud is very useful in understanding the need to understand the crucial elements of the privacy debate. Looking to the dark side of the Internet, it is clear that fraudsters like the Internet. First, it allows them to be more efficient and effective in what they do and creates difficulties for law enforcement in tracing transactions back to specific machines or addresses. Second, there has been a transposition of trust from the real world into the Internet world from consumers. In real terms, this amounts to companies losing 20 to 30 percent to fraud—numbers that can spell the end to companies given the tight margins in e-commerce. One recent statistic noted that fraud on the Internet represents 1.4 billion USD, or 11 percent of all e-commerce transactions. Thus, the most important engine to e-commerce fraud is that when you move from the real world to the virtual world, you can assume another identity that suits the fraudsters.

#### Crime hurts U.S. economy, competitiveness, and increases corruption in weak countries - $1 trillion every year

**NSC 11 –** National Security Council. (“Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security”, National Security Council, July 25, 2011, https://www.whitehouse.gov/administration/eop/nsc/transnational-crime)//chiragjain

Transnational organized crime (TOC) poses a significant and growing threat to national and international security, with dire implications for public safety, public health, democratic institutions, and economic stability across the globe. Not only are criminal networks expanding, but they also are diversifying their activities, resulting in the convergence of threats that were once distinct and today have explosive and destabilizing effects. This Strategy organizes the United States to combat TOC networks that pose a strategic threat to Americans and to U.S. interests in key regions. Penetration of State Institutions, Corruption, and Threats to Governance. Developing countries with weak rule of law can be particularly susceptible to TOC penetration. TOC penetration of states is deepening, leading to co-option in a few cases and further weakening of governance in many others. The apparent growing nexus in some states among TOC groups and elements of government—includ­ing intelligence services—and high-level business figures represents a significant threat to economic growth and democratic institutions. In countries with weak governance, there are corrupt officials who turn a blind eye to TOC activity. TOC networks insinuate themselves into the political process in a variety of ways. This is often accomplished through direct bribery (but also by having members run for office); setting up shadow economies; infiltrating financial and security sectors through coercion or corruption; and positioning themselves as alternate providers of governance, security, services, and livelihoods. As they expand, TOC networks may threaten stability and undermine free markets as they build alliances with political leaders, financial institutions, law enforcement, foreign intelligence, and security agen­cies. TOC penetration of governments is exacerbating corruption and undermining governance, rule of law, judicial systems, free press, democratic institution-building, and transparency. Further, events in Somalia have shown how criminal control of territory and piracy ransoms generate significant sums of illicit revenue and promote the spread of government instability. Threats to the Economy, U.S. Competitiveness, and Strategic Markets. TOC threatens U.S. economic interests and can cause significant damage to the world financial system through its subversion, exploi­tation, and distortion of legitimate markets and economic activity. U.S. business leaders worry that U.S. firms are being put at a competitive disadvantage by TOC and corruption, particularly in emerging markets where many perceive that rule of law is less reliable. The World Bank estimates about $1 trillion is spent each year to bribe public officials, causing an array of economic distortions and damage to legitimate economic activity. The price of doing business in countries affected by TOC is also rising as companies budget for additional security costs, adversely impacting foreign direct investment in many parts of the world. TOC activities can lead to disruption of the global supply chain, which in turn dimin­ishes economic competitiveness and impacts the ability of U.S. industry and transportation sectors to be resilient in the face of such disruption. Further, transnational criminal organizations, leveraging their relationships with state-owned entities, industries, or state-allied actors, could gain influence over key commodities markets such as gas, oil, aluminum, and precious metals, along with potential exploitation of the transportation sector. Crime-Terror-Insurgency Nexus. Terrorists and insurgents increasingly are turning to TOC to gener­ate funding and acquire logistical support to carry out their violent acts. The Department of Justice reports that 29 of the 63 organizations on its FY 2010 Consolidated Priority Organization Targets list, which includes the most significant international drug trafficking organizations (DTOs) threatening the United States, were associated with terrorist groups. Involvement in the drug trade by the Taliban and the Revolutionary Armed Forces of Colombia (FARC) is critical to the ability of these groups to fund terrorist activity. We are concerned about Hizballah’s drug and criminal activities, as well as indications of links between al-Qa`ida in the Lands of the Islamic Maghreb and the drug trade. Further, the terrorist organization al-Shabaab has engaged in criminal activities such as kidnapping for ransom and extortion, and may derive limited fees from extortion or protection of pirates to generate funding for its operations. While the crime-terror nexus is still mostly opportunistic, this nexus is critical nonetheless, especially if it were to involve the successful criminal transfer of WMD material to terrorists or their penetration of human smuggling networks as a means for terrorists to enter the United States.

## CHINA DISAD

### 1nc

#### China will likely require encryption backdoors now to assuage fears of rising internal unrest – BUT it’s uncertain – citing U.S. hypocrisy is key to resist pressure

Iasiello 15 (Emilio Iasiello, over 12 years’ experience as a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, published extensively in peer-reviewed journals, “China’s Anti-Terror Law May Be Bargaining Chip in Cyber Game,” 4-29-2015, http://darkmatters.norsecorp.com/2015/04/29/chinas-anti-terror-law-may-be-bargaining-chip-in-cyber-game/)

In March 2015, China’s Foreign Ministry said that deliberation on a controversial Chinese anti-terrorism law is going on and will be formulated based on national security needs,[i] refuting a senior U.S. official’s suggestion that the legislation was on hold. [ii] While this law has incurred significant criticism from the U.S. and other Western interests, China may try to use it to leverage bigger gains for itself in cyberspace discussions with Western interests. The New Law – for National Security, IP Exploitation, or Both? At the crux of the debate of the draft law is a requirement that would compel technology firms supplying technology to Chinese banks to install “backdoors” in products or relinquish sensitive information such as encryption keys to the government. The initial draft of the law, published by the National People’s Congress (NPC) late last year, requires companies to also keep servers and user data within China, supply law enforcement authorities with communications records and censor terrorism-related Internet content.[iii] The proposed law has received substantial criticism from Western countries to include Japan, the United States, and the European Union (EU) who have since engaged in collaboration to project a unified front against this draft law.[iv] According to a European Commission spokesperson, the EU is concerned by the lack of transparency in the development of these measures and by the potential impact on EU companies.[v] China has gone on the offensive to reduce the perception of any potential impropriety, addressing concerns publicly, and reiterating its stance that such legal actions are necessary antiterrorism measures to protect its national security interests. According to China, the law is ultimately justified in asking that technology companies make telecommunications and Internet ports accessible to the government for investigations,[vi] a sentiment similar to one that Federal Bureau of Investigation Director Comey expressed in 2014 when he said that government access to mobile devices may be needed in extreme circumstances, such as in the event of a terror attack.[vii] While fears of China being able to have access and exploit the intellectual property of IT companies, and possibly exploiting it for nefarious purposes is based on espionage activities attributed to Beijing, at least one leading U.S. company has agreed to submit to China’s restrictions,[viii] suggesting that gaining a foothold into a valuable marketplace may trump any security concerns. New Restrictions May Prove Win-Win for China Notably, China’s push for this law’s enactment comes at a time when China has received negative reactions to alleged cyber espionage allegations, to include the indictment of five of its military officers by the U.S. Department of Justice in 2014. Conversely, alleged National Security Agency documents leaked by Edward Snowden have provided China with ammunition to accuse the United States of similar, if not more sophisticated and global, activities. As a result, dialogue between the two governments has hit an impasse; the cybersecurity working group established in 2013 by the two governments has since been suspended by China with no indication of when discussions will continue. It remains uncertain if China will repeal or at least temper these restrictions, although as of March 31, they had agreed to suspend its rollout.[ix] Nevertheless, China has long desired to reduce its reliance on foreign technology, a long term science and technology plan that has been in effect since 2006.[x] If China goes forth with the cyber restrictions, forcing foreign technology companies to accede to its new security demands may prove a win-win deal for China. If companies do agree to its conditions, China will have access to proprietary code and customer information it may not have had as easy access to before. If the new restrictions end up deterring foreign technology from entering the Chinese IT market, Chinese companies will be able to assume a bigger role in supplying technology for its domestic customers. While these products may not be as advanced as Western counterparts, it will reduce the China’s own fears over the potential compromised technology produced by U.S. companies. Conclusion China may use the potential tweaking of this legislation before it’s enacted into law as a bargaining chip for other considerations it deems more pressing to its interests. Prior to this controversy, the U.S. had begun to review new trade agreements that limited the restrictions that can be put on the free flow of data across borders.[xi] The U.S. is currently negotiating with the EU and 20 other countries on a new agreement on services to guarantee the free flow of data across borders, a negotiation that China has been blocked from joining. [xii] Amending the wording on the current anti-terror law may provide China a seat at this table and allow it to influence this outcome, particularly as it views information control as an essential component for preserving political stability and keeping the regime in power.

#### The plan reinvigorates U.S. pressure on China – prevents backdoors and independently empowers dissidents

Bankston 15 (Kevin S. Bankston, Policy Director of the Open Technology Institute and Co-Director of Cybersecurity Initiative, New America, Security Fellow with the Truman National Security Project, serves on the board of the First Amendment Coalition, former Senior Counsel and the Director of the Free Expression Project at the Center for Democracy & Technology, former nonresidential fellow with the Stanford Law School’s Center for Internet & Society, former Senior Staff Attorney and Equal Justice Works/Bruce J. Ennis First Amendment Fellow at Electronic Frontier Foundation, former Justice William Brennan First Amendment Fellow, litigated Internet-related free speech cases at the American Civil Liberties Union, J.D. University of Southern California Law School, B.A. University of Texas at Austin, statement before the U.S. House of Representatives, Subcommittee on Information Technology of the Committee on Oversight and Government Reform, Hearing on “Encryption Technology and Possible U.S. Policy Responses,” 4-29-2015, <http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf>)

However, the free speech impact of a mandate against unbreakable encryption and in favor of backdoors for government would reach far beyond just the communication of encryption code, and chill a wide variety of online expression. When individuals believe that they may be under surveillance, there is a “chilling effect” that can curb free speech and the free flow of information online.59 If individuals must assume that their online communications are not secure but may instead be acquired by the U.S. government or by anyone else who might exploit an encryption backdoor, they will be much less willing to communicate freely. By contrast, encouraging the availability of strong encryption free of surveillance backdoors can enable free expression both in the United States and around the world, 60 including by stymieing the censorship and surveillance efforts of governments with less respect for human rights than our own. 8. It would encourage countries with poor human rights records to demand backdoor access of their own. The governments of countries like China, 61 India, 62 and the United Arab Emirates63 have proposed a variety of measures that would require companies to implement key escrow systems or other forms of backdoors or stop doing business in those countries, proposals that the United States government has criticized.64 Yet how can the United States credibly criticize, for example, the Chinese government for proposing an anti-terrorism bill that would require U.S. companies to hand over their encryption keys, if we impose a similar requirement here at home? And how are U.S. companies to argue that they cannot implement such requirements and hand over the keys to foreign governments—even those with a history of human rights abuses—if they have already had to do so for the U.S. government? As Marc Zwillinger has pointed out, if the U.S. mandates backdoor access to encrypted data, “multinational companies will not be able to refuse foreign governments that demand [the same] access. Governments could threaten financial sanctions, asset seizures, imprisonment of employees and prohibition against a company’s services in their countries. Consider China, where U.S. companies must comply with government demands in order to do business.” 65 Such a result would be particularly ironic considering the U.S.’s foreign policy goal of promoting Internet Freedom worldwide and in China especially, including the promotion of encryption-based tools to protect privacy and evade censorship.66 Internet Freedom begins at home, and a failure by the United States to protect Americans’ ability to encrypt their data will undermine the right to encrypt and therefore human rights around the world. 67 The U.S. government supports the use of strong encryption abroad as part of our foreign policy objectives, and it should support the same for Americans here in the United States. This is especially true considering that…

#### Fear of unrest causes lashout and extinction

Renxing 5 (San Renxing, writer for the free republic, Epoch Times international, “CCP Gambles Insanely to Avoid Death,” 8-3-2005, <http://www.theepochtimes.com/news/5-8-3/30931.html>)

Since the Party’s life is “above all else,” it would not be surprising if the CCP resorts to the use of biological, chemical, and nuclear weapons in its attempt to postpone its life. The CCP, that disregards human life, would not hesitate to kill two hundred million Americans, coupled with seven or eight hundred million Chinese, to achieve its ends. The “speech,” free of all disguises, lets the public see the CCP for what it really is: with evil filling its every cell, the CCP intends to fight all of mankind in its desperate attempt to cling to life. And that is the theme of the “speech.” The theme is murderous and utterly evil. We did witness in China beggars who demanded money from people by threatening to stab themselves with knives or prick their throats on long nails. But we have never, until now, seen a rogue who blackmails the world to die with it by wielding biological, chemical, and nuclear weapons. Anyhow, the bloody confession affirmed the CCP’s bloodiness: a monstrous murderer, who has killed 80 million Chinese people, now plans to hold one billion people hostage and gamble with their lives.

### a2 no brink

#### CCP legitimacy at tipping point—organized protests topples the regime

Ong 15 (Lynette H. Ong Associate Professor of Political Science at the University of Toronto, jointly appointed by the Department of Political Science and the Asian Institute, Munk School of Global Affairs, and China Specialist at the University of Toronto. Postdoctoral Fellow at Harvard University’s Fairbank Center for Chinese Studies. “Chinese Regime stability: sustaining or collapsing?” Asia Pacific Foundation. https://www.asiapacific.ca/canada-asia-agenda/chinas-regime-stability-sustaining-or-collapsing, June 2, 2015)\\mwang

Attacks outside the party: "Stability preservation" Shortly after Xi assumed the presidency in 2012, he shifted the locus of power to the newly created National Security Commission, which is tasked with overseeing both foreign affairs and domestic security. Xi chairs this powerful commission himself, which allowed him to concentrate his control over internal security resources and of removing any potential powerful contender within the upper echelons of the party in charge of this portfolio. The result has been an increase in the scope, targets and intensity of political repression of society. The party's coercive apparatus, or "stability preservation" (weiwen), to use the official rhetoric, expanded significantly under Hu Jintao, though its origins date back to the post-1989 crackdown. But the scope of the coercive apparatus has widened even further to include Internet monitoring and censorship**,** the Public Security Bureau, the policy and state intelligence agencies, the People's Armed Police, the paramilitary forces, local "stability-maintenance units," and urban patrols or chengguan. In addition, Xi inherited a budget for "stability preservation" that reportedly increased more than five-fold between 2002 and 2012, from 132.8 billion yuan (US$16.2 billion) to 702 billion yuan ($111 billion), exceeding the officially published military budget. A recent Freedom House report notes that a wide range of groups have experienced an increase in repression since 2013, including grassroots rights activists, online opinion leaders, internet users, business people, party cadres, labour leaders, scholars and professors, print and television journalists, Christians, Tibetans and Uighurs. And Document No. 9, issued by the Central Committee in 2013, ordered all relevant institutions to stem any endorsement of universal "Western" values, such as media freedom, civil society and judicial independence. Reaching a turning point? The harsh crackdown has also been applied to commercial media and social media. The Central Internet Security and Informational Leading Group was set up in 2014 to coordinate work on cyber security and internet censoring. Internet censoring used to be largely outsourced to Internet companies that keep an eye on their users. This new leading group, also headed by Xi, indicates that information control is a high priority. The filtering and management of content is now increasingly centrally controlled and coordinated. The once-fiery Southern Weekly, which had served as the leading example of commercialized media pushing the envelope of press freedom, has largely lost its luster. Online opinion leaders, such as blogger Murong Xuecun, who had millions of followers on social media, saw their freedom of speech significantly curtailed. Sina Weibo, the equivalent of Twitter in China, which was once a platform for raucous discussion of social issues, has also quieted down. Ordinary Internet users across the areas of businesses, academia, and journalism have lamented that the Internet in China has largely become an Intranet. Yet, the intensified Internet censorship and crackdown on social media have not intimidated the Chinese netizens. An increasing number of Internet users in China are using Virtual Private Networks and other circumvention tools to scale the "Great Firewall." Xiao Qiang of the China Digital Times at the University of California at Berkeley argues that the crackdown has emboldened Internet users to seek alternative ways to express their opinions, rather than injecting fear among them. The crackdown has also increased resentment against the censorship apparatus. Freedom House has observed civil society resilience amid the crackdowns. Some civil society organizations might have been pushed underground, but they are not giving up the fight for their causes. Repression has strained state-society relations and led to declining regime legitimacy. Although citizens may not have the resources or mobilizing structures to organize large-scale collective action, it is nonetheless significant that the grievances that motivate them to do so are now stronger than ever before. After the Tiananmen incident in 1989, there was an implicit social contract in which citizens agreed to political acquiescence in exchange for the regime's delivery of economic prosperity. So far, the regime has largely held up its end of the deal: Real income for the urban middle class has been rising, though housing affordability is a major concern, and wages of migrant workers have risen sharply in the last decade, making them significantly better off than a generation ago. However, with slower economic growth, the regime's ability to maintain performance legitimacy now comes under increased scrutiny. This scrutiny, coupled with the falling regime legitimacy from the intensified crackdown, seems to be bringing the populace closer to the breaking point than any period after 1989. In essence, Xi is implementing harsh repression within as well as outside the system. Thus far, he seems to have the support of the other members of the Politburo Standing Committee, the apex of the party's power. But, the anti-corruption campaign is having chilling effects on bureaucrats, party rank-and-file and leaders across all levels. They constantly live in fear under the current political climate. The fact that some of them have become disenfranchised with the party leadership was not unforeseeable. Yet, they are also the very implementers of Xi's repressive actions on those outside the system. This makes the simultaneous timing of both repressive measures unwise, at least from the perspective of party preservation. If there is a common cause or interest around which those within and outside the system could cooperate, threats to the regime will mount. Freedom House's interviews with activists suggest some security agents have decided not to enforce their superior's instructions strictly out of sympathy or conscience.

### a2 no lashout

#### Chinese Instability escalates to CCP lashout

**Shirk, expert on Chinese politics, 2007**

(Susan L. Shirk, expert on Chinese politics and former Deputy Assistant Secretary of State during the Clinton administration, also in the Bureau of East Asia and Pacific Affairs, and professor at the Graduate School of International Relations and Pacific Studies at the University of California in San Diego, “China Fragile Superpower” published by Oxford University Press, Chapter 3, page 69.) // RL

As China’s leaders well know, the greatest political risk lying ahead of them is the possibility of an economic crash that throws millions of workers out of their jobs or sends millions of depositors to withdraw their savings from the shaky banking system. A massive environmental or public health disaster also could trigger regime collapse, especially if people’s lives are endangered by a media cover-up imposed by Party authorities. Nationwide rebellion becomes a real possibility when large numbers of people are upset about the same issue at the same time. Another dangerous scenario is a domestic or international crisis in which the CCP leaders feel compelled to lash out against Japan, Taiwan, or the United States because from their point of view not lashing out might endanger Party rule.

### a2 collapse inevitable

#### China legitimacy high now

Jacques 12 (Martin Jacques is an economist and author of When China Rules the World. BBC news. “A Point Of View: Is China more legitimate than the West?” <http://www.bbc.com/news/magazine-20178655> November 12, 2012)\\mwang

China and the United States are about to choose new leaders via very different methods. But is a candidate voted for by millions a more legitimate choice than one anointed by a select few, asks Martin Jacques. This week will witness an extraordinary juxtaposition of events. On Tuesday the next American president will be elected. Two days later, the 18th congress of the Chinese Communist Party will select the new Chinese president and prime minister. The contrast could hardly be greater. Americans in their tens of millions will turn out to vote. In China the process of selection will take place behind closed doors and involve only a relative handful of people. You are probably thinking, "Ah, America at its best, China at its worst - the absence of democracy. China's Achilles heel is its governance. This will be China's downfall." I want to argue quite the contrary. You probably think that the legitimacy and authority of the state, or government, is overwhelmingly a function of democracy, Western-style. But democracy is only one factor. Nor does democracy in itself guarantee legitimacy. A Point of View broadcasts on BBC Radio 4 on Fridays at 20:50 GMT and repeated on Sunday at 08:50 GMT Think of Italy. It is always voting, but the enduring problem of Italian governance is that its state lacks legitimacy. Half the population don't really believe in it. Now let me shock you: the Chinese state enjoys greater legitimacy than any Western state. How come? In China's case the source of the state's legitimacy lies entirely outside the history or experience of Western societies. In my first talk I explained that China is not primarily a nation-state but a civilisation-state. For the Chinese, what matters is civilisation. For Westerners it is nation. The most important political value in China is the integrity and unity of the civilisation-state. Given the sheer size and diversity of the country, this is hugely problematic. Between the 1840s and 1949, China was occupied by the colonial powers, divided and fragmented. The Chinese refer to it as their century of humiliation. They see the state as the embodiment and guardian of Chinese civilisation. Its most important responsibility - bar none - is maintaining the unity of the country. A government that fails to ensure this will fall. There have been many examples in history. The legitimacy of the Chinese state lies, above all, in its relationship with Chinese civilisation. But does the Chinese state, you may well ask, really enjoy legitimacy in the eyes of its people? Take the findings of Tony Saich at Harvard's Kennedy School of Government. In a series of surveys he found that between 80 and 95% of Chinese people were either relatively or extremely satisfied with central government.Chinese people say they are happy with their government's economic record Or take the highly respected Pew Global Attitudes surveys which found in 2010, for example, that 91% of Chinese respondents thought that the government's handling of the economy was good (the UK figure, incidentally was 45%). Such high levels of satisfaction do not mean that China is conflict-free. On the contrary, there are countless examples of protest action, such as the wave of strikes in Guangdong province for higher wages in 2010 and 2011, and the 150,000 or more so-called mass incidents that take place every year - generally protests by farmers against what they see as the illegal seizure of their land by local authorities in cahoots with property developers. But these actions do not imply any fundamental dissatisfaction with central government. If the Chinese state enjoys such support, then why does it display such signs of paranoia? The controls on the press and the internet, the periodic arrest of dissidents, and the rest of it. Good point. Actually, all Chinese governments have displayed these same symptoms. Why? Because the country is huge and governance is extremely difficult. They are always anxious, always fearing the unforeseen. Anticipating sources of instability has long been regarded as a fundamental attribute of good governance. Not surprisingly, the Chinese have a quite different attitude towards government to that universal in the West. True, our attitude depends in part on where we stand on the political spectrum. If you are on the right, you are likely to believe in less government and more market. If you are on the left, you are likely to be more favourably disposed to the state. But both left and right share certain basic assumptions. The role of the state should be codified in law, there should be clear limits to its powers, and there are many areas in which the state should not be involved. We believe the state is necessary - but only up to a point. The Chinese idea of the state could hardly be more different. The Chinese see the state as a member of the family - the head of the family, in fact They do not view it from a narrowly utilitarian standpoint, in terms of what it can deliver, let alone as the devil incarnate in the manner of the American Tea Party. They see the state as an intimate, or, to be more precise, as a member of the family - the head of the family, in fact. The Chinese regard the family as the template for the state. What's more, they perceive the state not as external to themselves but as an extension or representation of themselves. The fact that the Chinese state enjoys such an exalted position in society lends it enormous authority, a remarkable ubiquity and great competence. Take the economy. China's economic rise - an annual growth rate of 10% for more than 30 years - has been masterminded by the Chinese state. It is the most remarkable economic transformation the world has seen since the modern era began with Britain's industrial revolution in the late 18th Century. Even though China is still a poor developing country, its state, I would argue, is the most competent in the world. Take infrastructure - the importance of which is belatedly now being recognised in the West. Here, China has no peers. Its high speed rail network is the world's largest and will soon be greater than the rest of the world's put together. And the state's ubiquity - a large majority of China's most competitive companies, to this day, are state-owned. Or consider the one-child policy, which still commands great support amongst the population. The competence of the state is little talked about or really valued in the West, especially in the Anglo-Saxon world. Indeed, since the early 80s, the debate about the state in Britain has largely been conducted in terms either of what bits should be privatised or how it can be made to mimic the market. Now, however, we are in a new ball game. With the Western economies in a profound mess and with China's startling rise, the competence of the state can no longer be ignored. Our model is in crisis. Theirs has been delivering the goods. As China's dramatic ascent continues - which it surely will - then China's strengths will become a growing subject of interest in the West. We will realise that our relationship with them can no longer consist of telling them how they should be like us. A little humility is in order. One of the most dramatic illustrations of this will be the state. We think of it as their greatest weakness but we will come to realise that it is one of their greatest strengths. Beyond a point it would be quite impossible for a Western state to be like China's. It is the product of a different history and a different relationship between state and society. You could never transplant their state into a Western country, and vice versa. But this does not mean that we cannot learn from the Chinese state, just as they have learnt much from us. China's rise will have a profound effect on Western debate. The Chinese economy is set to overtake the US in 2018 In about six years hence, the Chinese economy will overtake the US economy in size. By 2030 it will be very much larger. The world is increasingly being shaped by China, and if it has looked west for the last two centuries, in future it will look east. Welcome, then, to the new Chinese paradigm - one that combines a highly competitive, indeed often ferocious market, with a ubiquitous and competent state. For us in the West this is an entirely new phenomenon. And it will shape our future.

### a2 no collapse

#### China is close, but won’t collapse now: legitimacy high

Tao 15 (Xie Tao,professor of political science at the School of English and International Studies, Beijing Foreign Studies University. He holds a PhD in political science from Northwestern. “Why do people keep predicting China’s Collapse?” The Diplomat. <http://thediplomat.com/2015/03/why-do-people-keep-predicting-chinas-collapse/> March 2015)\\mwang

The temptation to make predictions about China is probably irresistible, because it is arguably the most important contemporary case in international relations. Thus, a few Western observers have risked their professional reputations by acting as prophets. Perhaps the most (in)famous is Gordon Chang, who published The Coming Collapse of China in 2001. “The end of the modern Chinese state is near,” he asserted. “The People’s Republic has five years, perhaps ten, before it falls,” China didn’t collapse, as we all know. “So, yes, my prediction was wrong,” he admitted in an article (“The Coming Collapse of China: 2012 Edition”). But he remained convinced about the imminence of a Chinese apocalypse and offered a new timeline: “Instead of 2011, the mighty Communist Party of China will fall in 2012. Bet on it.” Gordon Chang may be dismissed as an opportunist who tries to make a fortune — political and/or economic — out of sensational rhetoric about China. But not so with David Shambaugh, a well-respected China scholar at George Washington University who heretofore has been rather cautious in his assessment of China. In a March 6 Wall Street Journal article, he portrayed the Chinese party-state as struggling for its last breath. “The endgame of Chinese communist rule has now begun, I believe, and it has progressed further than many think,” he wrote. “We cannot predict when Chinese communism will collapse, but it is hard not to conclude that we are witnessing its final phase.” Shambaugh’s article was nothing less than a supersize bombshell in the China field, especially in light of the fact that the Chinese Communist Party under Xi Jinping’s leadership seems to be revitalizing itself through a series of important measures. And these measures — particularly the anti-corruption campaign and the drive for the rule of law — appear to have significantly bolstered popular support for the new leadership. Shambaugh actually published a book in 2008 that offers a rather favorable assessment of the party-state’s abilities to adapt to new challenges in the first decade of the 21st century. It is unclear what caused Shambaugh’s sudden about-face. Some speculate that he was merely trying to get a foreign policy position in the post-Barack Obama administration. Others contend that he is the Chinese version of a “mugged” liberal converted to a conservative, that Shambaugh is deeply upset by Chinese leaders’ intransigence on fundamental reforms. Whatever the motives behind Shambaugh’s nirvana, there is no denying that China is facing myriad daunting challenges. China is sick — but so is every other country in the world, though each country is sick with different symptoms, for different reasons, and of different degrees. Take the United State as an example. The world’s oldest democracy may also strike one as terminally ill: appalling inequality, dilapidated infrastructure, declining public education, astronomical deficits, rising political apathy, and a government that can hardly get anything done. In his bestseller Political Order and Political Decay, Francis Fukuyama described the American body politic as being repatrimonialized, ruled by courts and political parties, and gridlocked by too many veto points. Across the Atlantic, many European democracies are facing similar problems, particularly financial insolvency. Yet nobody has declared the coming collapse of American democracy or European democracy. Why? Because many Western analysts (dating back at least to Seymour Martin Lipset) subscribe to the view that as long as political institutions are viewed as legitimate, a crisis in effectiveness (e.g., economic performance) does not pose fatal threat to a regime. Thus even in the darkest days of the Great Depression, according to this view, America’s democratic institutions remained unchallenged. By contrast, if a regime is already deficient in political legitimacy, a crisis of effectiveness (such as an economic slowdown, rising inequality, or rampant corruption) would only exacerbate the legitimacy crisis. China is widely believed to be a prominent case that fits into this line argument. China might be facing a performance crisis, but whether it is also facing a legitimacy crisis is debatable. Beauty is in the eyes of beholder; so is legitimacy. If the Chinese party-state could survive the riotous years of the Cultural Revolution and the existential crisis of 1989, why couldn’t it manage to survival another crisis? In fact, a more important question for Western observers is why the Chinese Communist Party has managed to stay in power for so long and to produce an indisputably impressive record of economic development.

### a2 backdoors not key

#### Backdoors needed for China cybersecurity

Kan 15 (Micheal Kan, covers IT, telecommunications, and the Internet in China for the IDG News Service, Beijing Correspondent. “China Defends Cybersecurity back door demands as Obama protests.” PC world, IGD News Service. [http://www.pcworld.com/article/2892052/china-defends-cybersecurity-demands-amid-complaints-from-us.html March 3](http://www.pcworld.com/article/2892052/china-defends-cybersecurity-demands-amid-complaints-from-us.html%20March%203), 2015)\\mwang

President Barack Obama isn’t happy with new rules from China that would require U.S. tech companies to abide by strict cybersecurity measures, but on Tuesday the country was quick to defend the proposed regulations. “All countries are paying attention to and taking measures to safeguard their own information security. This is beyond reproach,” said China’s Foreign Ministry spokesman Hua Chunying in a news briefing. She made the statement after Obama criticized a proposed anti-terror law that he said could stifle U.S. tech business in China. The legislation would require companies to hand over encryption keys to the country’s government, and create “back doors” into their systems to give the Chinese government surveillance access. “This is something that I’ve raised directly with President Xi,” Obama said in an interview with Reuters on Monday. “We have made it very clear to them that this is something they are going to have to change if they are to do business with the United States.” A fight over intellectual property U.S. trade groups are also against another set of proposed regulations that would require vendors selling to China’s telecommunication and banking sector to hand over sensitive intellectual property to the country’s government. Although China hasn’t approved the proposed regulations, the country has made cybersecurity a national priority over the past year. This came after leaks from U.S. National Security Agency contractor Edward Snowden alleged that the U.S. had been secretly spying on Chinese companies and schools through cyber surveillance. On Tuesday, China signaled that there was a clear need to protect the country from cyber espionage. Foreign Ministry spokeswoman Hua pointed to recent reports alleging that the U.S. and the U.K. had hacked into a SIM card maker for surveillance purposes as an example. “I would like to point out that **China has consistently opposed using one’s superiority in information technology, or using IT products to support cyber surveillance,**” she said, adding that the anti-terror legislation relates to the country’s domestic affairs. China already imposes tough regulations on U.S. tech businesses through its strict online censorship that has blocked websites such as Facebook and Twitter. But last May, the country announced it was developing a new “cybersecurity vetting system” meant to weed out secret spying activities. Companies that failed to pass the vetting would be blocked from the market.

### a2 no modeling

#### US backdoors in encryption spill-over to Chinese backdoors

**Mason, white house correspondent, quoting president Obama, 3/2**/15

(Jeff Mason, lead white house correspondent for Obama’s 2012 campaign and posted in Washington since 2008, Reuters, <http://www.reuters.com/article/2015/03/02/us-usa-obama-china-idUSKBN0LY2H520150302>) // RL

President [Barack Obama](http://www.reuters.com/people/barack-obama) on Monday sharply criticized China's plans for new rules on U.S. tech companies, urging Beijing to change the policy if it wants to do business with the United States and saying he had raised it with President Xi Jinping. In an interview with Reuters, Obama said he was concerned about Beijing's plans for a far-reaching counterterrorism law that would require technology firms to hand over encryption keys, the passcodes that help protect data, and install security "backdoors" in their systems to give Chinese authorities surveillance access. "This is something that I’ve raised directly with President Xi," Obama said. "We have made it very clear to them that this is something they are going to have to change if they are to do business with the United States." The Chinese government sees the rules as crucial to protect state and business secrets. Western companies say they reinforce increasingly onerous terms of doing business in the world's second-largest economy and heighten mistrust over cybersecurity between Washington and Beijing. A Chinese parliamentary body read a second draft of the country's first anti-terrorism law last week and is expected to adopt the legislation in the coming weeks or months. The initial draft, published by the National People's Congress late last year, requires companies to also keep servers and user data within [China](http://www.reuters.com/places/china), supply law enforcement authorities with communications records and censor terrorism-related Internet content. The laws "would essentially force all foreign companies, including U.S. companies, to turn over to the Chinese government mechanisms where they can snoop and keep track of all the users of those services," Obama said. "As you might imagine tech companies are not going to be willing to do that," he said. The scope of the rules reaches far beyond a recently adopted set of financial industry regulations that pushed Chinese banks to purchase from domestic technology vendors. The implications for Silicon Valley companies, ranging from Microsoft Corp ([MSFT.O](http://www.reuters.com/finance/stocks/overview?symbol=MSFT.O)) toApple Inc ([AAPL.O](http://www.reuters.com/finance/stocks/overview?symbol=AAPL.O)), have set the stage for yet another confrontation over cybersecurity and technology policy, a major irritant in U.S.-China relations. Obama said the rules could also backfire on China. "Those kinds of restrictive practices I think would ironically hurt the Chinese economy over the long term because I don’t think there is any U.S. or European firm, any international firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government," he said. A U.S. official told Reuters last week that the Obama administration has conveyed its concerns about the anti-terrorism draft law to China. REGULATORY PRESSURE Although the counterterrorism provisions would apply to both domestic and foreign technologies, officials in Washington and Western business lobbies argue the law, combined with the new banking rules and a slew of anti-trust investigations, amount to unfair regulatory pressure targeting foreign companies. To be sure, Western governments, including in the United States and Britain, have for years requested tech firms to disclose encryption methods, with varying degrees of success. Officials including FBI director James Comey and National Security Agency (NSA) director Mike Rogers publicly warned Internet companies including Apple and [Google](http://www.reuters.com/finance/stocks/overview?symbol=GOOG.O) late last year against using encryption that law enforcement cannot break. Beijing has argued the need to quickly ratchet up its cybersecurity measures in the wake of former NSA contractor Edward Snowden's revelations of sophisticated U.S. spying techniques. China is drafting the anti-terrorism law at a time when Chinese leaders say the country faces a serious threat from religious extremists and separatists. Hundreds of people have been killed over the past two years in the far-western region of Xinjiang in unrest the government has blamed on Islamists who want to establish a separate state called East Turkestan.