A Repertory of Cyber Analogies

Robert Axelrod
Ford School of Public Policy, University of Michigan
axe@umich.edu

October 21, 2013

A report prepared for the CyberCom Project on Cyber Analogies

Abstract: This report provides a repertory of 35 analogies that can be relevant to issues related to cyber conflict. Analogies such as these can serve several purposes: to motivate (by fear or inspiration), to demonstrate what is possible, to provide examples from the past of things to avoid, and to illuminate particular features of past events that might be worth thinking about in preparation for cyber conflict. The report provides the implications of each analogy. These implications can be thought of as lessons from the past that can be useful once again, despite important changes in technology, doctrine, organization and political context. The analogies are organized in sections on historical analogies from before, during and after World War II, and a section on functional analogies such as those inspired by biology. The report includes an appendix on a tactic that has been used by the Chinese that is quite distinct from Western conceptions of deterrence, namely the denial of retaliatory intent.

Acknowledgments: I wish to thank all the participants in the CyberCom Project on Cyber Analogies, and especially Emily Goldman, Keith Alexander, and Dorothy Denning. This work was done with financial support from the Air Force Office of Scientific Research Grant FA9550-10-1-0373 and CyberCom.

A. Before World War II

1. David and Goliath

Implication: Asymmetric warfare can topple a giant. The religious significance of the story is somewhat different, namely that overwhelming odds can be overcome if God is on one's side. For many Muslims, the Soviet defeat in Afghanistan is a clear example of David and Goliath.

2. "Remember the Maine"

Implication: Destruction of a military target can lead to jingoism and be used to justify war, even if the destruction could have been an accident. In 1898, the U.S.S. Maine exploded in Havana Harbor, leading to the battle cry of "Remember the Maine, to Hell with Spain!" The exploitation of this event in the American press helped launch the Spanish-American War. The lesson for the cyber realm is that the meaning of an ambiguous event can be shaped by the media to appear to be a deliberate provocative act, resulting in a demand for an overwhelming response. In the case of China, the national media is controlled by the regime, but when the indignation of ultra-nationalist micro bloggers resonates with the broader public, the resulting pressure on the government could be intense. (See also Gulf of Tonkin Incidents.)

3. Demise of Piracy

Implication: Major powers working together can eliminate private attempts to do damage to the global economy, e.g. by holding companies hostage. On the other hand, territories without proper governance (whether geographic or virtual) can be havens for piracy.

4. Privateering

Implication: Some activities that look like piracy might be legally sponsored by a nation, as specified in the U.S. Constitution. "Marque and reprisal — would the latter-day equivalent be to empower cyber-privateers in this way to go after certain targets…The possibility of cyber militias comes to mind as well (the Chinese are actually encouraging the formation of these).[1]"

5. Unrestricted Submarine Warfare

Implication: A tactic that begins by being regarded as "sneaky" and dishonorable can become accepted, as unrestricted submarine warfare was during the course of World War I. Observing the requirement to warn ships about to be attacked eliminated the value of the submarine, which is why giving warning was abandoned.[2] Of course, on the way to becoming accepted, the dishonorable tactic can contribute to an overwhelming hostile response. For example the German declaration of unrestricted submarine warfare contributed to the American decision to enter World War I. The lesson for cyber conflict

[1] John Arquilla, personal communication.
[2] Nicholas Lambert, personal communication.

is that new modes of attack are often seen as dishonorable, and therefore elicit stronger responses than would otherwise be expected.

6. Unanticipated Information Requirements for British Economic Warfare in World War I

Implication: The implementation of a policy may require information in ways not anticipated in peacetime. At the outset of World War I, when Britain tried to implement economic warfare against Germany, it was found that the information collected in peacetime was not always what was needed for wartime. In addition, even when the information *was* collected, it was often distributed over many different parts of the government (and the private sector) in ways that made it impossible to aggregate in a timely way. The difficulties of aggregation included incompatibilities of definitions, periods covered, and formats in which the data is kept. There was the additional problem of withholding information for competitive reasons (either profit or bureaucratic power), as well as legal constraints on sharing.[3]

7. Collateral Damage in British Economic Warfare in World War I

Implication: Collateral damage may require restrictions in the use of an otherwise successful form of warfare. Prior to World War I, the British Admiralty had plans to exploit Britain's dominant position in global trade and finance to strangle Germany and its allies at the outbreak of war. When war came, the policy was implemented, but it turned out to be impossible to strangle Germany without impinging on neutral rights in a manner highly provocative to the United States.[4] U.S. cyber measures could hurt allies and neutrals in a conflict (e.g. Japan or EU) so much that the U.S. would have to call off its attack, just as UK had to. An example might be if a conflict that included cyber attacks left only limited bandwidth that was fully secure (say because it went through the latest generation of communications satellites). Then one could imagine that the Pentagon would want to commandeer virtually all of it, but our own private sector and our allies would demand some for themselves.

B. During World War II

8. Blitzkrieg

Implication: New doctrine is as important as new technology. The French in 1940 had tanks, airplanes and radios, but only the Germans had the doctrine to take advantage of it.

9. Battle of Britain

Implication: A conflict could take place entirely within a single domain, such as air-to-air combat or cyberspace. "The analogous conflict in cyberspace would be a standalone, overt cyber battle or war between nations, fought entirely within the domain of cyberspace and fully engaging each side's cyber attackers and defenders (probably

[3] Lambert, Nicholas A. 2012. *Planning Armageddon: British Economics Warfare and the First World War*. Cambridge: Harvard University Press.

[4] Lambert, Nicholas A. 2012. *Planning Armageddon: British Economics Warfare and the First World War*. Cambridge: Harvard University Press.

both in government and the private sector). Though tactical engagements might take place "at the speed of light" these would be mere dogfights in the context of the larger fight, with complete operations as part of offensive and defensive campaigns. A cyber Battle of Britain may develop slowly, through various phases (as did the original, 70 years ago) moving up from smaller, less-organized attacks before blossoming into a full force-on-force unleashing of violence. Each side may be deterred from making larger cyber attacks (as the Germans originally forfeited attacking cities) but continue to one-up the other nation in a progression of violence."[5]

10. Fort Eban Emael

Implication: When design criteria are specified too narrowly a supposedly well-designed defense can be easily overcome. On May 10, 1940, seventy-seven Germans in gliders descended on Belgium's strongest fort, Eban Emael. Within a day, they had taken decisive steps to capture the garrison of 1200. The fort was well "buttoned up" and protected by massive casements and embrasures, being optimized against heavy attack from a distance. To the Belgians, worried about a heavy attack from a distance, gliders were an unknown unknown. Had the Belgians considered an attack from gliders directly onto the fort as even a very unlikely possibility, they could have easily taken measures to defeat a few dozen fully exposed soldiers.[6]

11. *Die Glückliche Zeit* (Golden Time)

Implication: At the start of a major conflict one side might present numerous easy targets until it adapts. The term *Die Glückliche Zeit* (Golden Time) is the German term for the period in the first summer of World War II when their submarines were able to sink 282 Allied ships.[7] The Second Happy Time was the summer after the U.S. entered WW II when German subs were able to sink 609 ships totaling more than three millions tons, roughly a quarter of the tonnage they sunk in the entire war.[8] This is an example of

> the 'harbor lights' phenomenon: when the U.S. entered WWII, it kept eastern seaboard cities' lights on after dark, illuminating targets for U-boats. The lights stayed on for fear of the economic consequences of blackout — and blackout was only imposed when U-boat depredations became too costly. A bit like the cyber security problem today. The harbor lights are on all over cyberspace, but the hacker/U-boat captains haven't done enough damage yet to cause more serious security measures to be taken.[9]

12. Battle of Taranto

Implication: Vulnerabilities in ones defense can be revealed by observing how a similar defense was overcome in another setting. On November 11, 1940, British torpedo

---

[5] Adapted Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use" in Proceedings of a Workshop on Deterring CyberAttacks, Committee on Deterring Cyberattacks, National Research Council. 2010. http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_059437.pdf

[6] See references in the Wikipedia article on "Fort Eben-Emael".

[7] See http://ww2db.com/battle_spec.php?battle_id=277

[8] See sources at http://en.wikipedia.org/wiki/Second_Happy_Time

[9] John Arquilla personal communication

planes overcame the defenses of the Italian battleships at Taranto by adapting their torpedoes to be effective in shallow waters.[10] Nevertheless, the American Navy failed to learn form this surrogate experience, so the battleships at Pearl Harbor remained vulnerable to Japanese torpedo plane attack.

13. Pearl Harbor

Implication: The trauma of Pearl Harbor means that the U.S. will always be alert to the possibility of a "bolt from the blue," even though Pearl Harbor itself was hardly an example of one. In fact, an important lesson of Pearl Harbor (and many other surprise attacks) is that a country can be surprised by the nature of the attack, but is almost never attacked without days, if not weeks, of a serious political crisis makes war a real possibility in the near future.[11] The implication for cyber war is that even though a cyber attack can be launched without tactical warning, it is very likely that any major attack will only happen in the context of a serious political crisis. An important lesson is that a potential target of a major cyber attack should be prepared to take advantage of the time available in a crisis to upgrade defensive capabilities in ways may not be practical in ordinary times. Of course, there may be political constraints on taking any measures that could be seen by the other side as preparations for a preemptive attack.[12]

C. After World War II

14. China Crosses the Yalu

Implication: Sometimes attacks are made at the start of a conflict, and then quickly stop. The natural interpretation of the target is that the attack was halted when its initial efforts were thwarted by effective defenses. However, another possibility is that the attacker planned all along that the attack would be launched and then halted in order to send a warning. The attack might have been meant as a demonstration of willingness to resort to this type of attack, and the pause might be designed to give the other side a last chance to avoid a more serious conflict.

In the autumn of 1950 as the United States forces were routing the North Korean Army and racing toward the Yalu River border with China, the Chinese tried to warn by both public and private messages that approaching the border would not be tolerated. The Chinese first sent troops over the Yalu to make contact with U.S. forces, and then deliberately broke contact. The U.S. did notice this but did not see it as a warning, despite

[10] Angelo N. Caravaggio, 2006. "The Attack at Taranto," *Naval War College Review*, vol. 59, no. 3. Pp. 103-127.

[11] Other well-known surprises support this point. For example, the U.S. was surprised by China's entry into the Korean War, but see item 14. Stalin was surprised by Hitler's attack, but that was because Stalin discounted the extensive evidence he had that an attack was imminent. Israel was surprised in 1973, but it too had sufficient warning that its leaders chose to discount. In all these cases, the attacks were preceded by days, if not weeks, of a serious political crisis that made war a real possibility in the near future.

[12] Alternatively, conspicuous preparations for escalation can sometimes help *deter* the other side from pursuing the conflict. For example in the Cuban Missile Crisis, the conspicuous preparation the U.S. undertook to invade Cuba was one of the main reasons why Khrushchev decided to end the crisis by withdrawing the missiles.

other numerous diplomatic and public attempts by the Chinese to warn the U.S. that it was about to intervene unless the U.S. backed off.[13]

The Chinese did the same thing against India in 1962, and against Vietnam in 1979.[14] In all three cases, the Chinese warned, then struck in a restrained manner, then paused, and - when their warnings were not heeded - they attacked in strength.[15] I know of no other country that has used this tactic.

The lesson is that when a cyber attack is halted, there are three possible interpretations: the attack failed, the attack was meant as a warning but was actually a bluff, and the attack was meant as a warning and was not a bluff. Especially if the attack comes from China, the third possibility needs to be taken seriously. [See also the Appendix.]

15. Vietnam and the Tet Offensive

Implication: A cyber attack could take the form of guerrilla warfare involving a few large-scale incidents with large-scale effects, but a continuing string of attrition attacks seeking to erode an adversary's power, influence, and will. A typical tactic of guerillas is to cause an overreaction from the other, more powerful, adversary as this can help push more people to supporting the guerillas' cause. Another is to ensure civilians are impacted directly or indirectly to force them to pressure their government to cease hostilities or influence the way the war is fought. In a true "cyber Vietnam" the attacking group would also have the backing of a national sponsor, aiding and encouraging its campaigns, though possibly unwilling to commit their own cyber or traditional military forces.[16] The massive Tet Offensive of 1968 was based on the premise that the urban population would rise up against the Saigon government if given the chance. The premise turned out to be wrong and the immediate result was the decimation of the Viet Cong. But the Tet Offensive had the unforeseen and possibly decisive effect of undermining the will of the American public to prosecute the war. The lesson for cyber attacks is that the effects may be important without being foreseen.

16. The Gulf of Tonkin Incidents

Implication: Seemingly solid information that an attack happened might have been subject to bureaucratic processes that filter out contradictory information, leading to the same result as if the attack had happened. The first incident in the Gulf of Tonkin was an attack on a U.S. destroyer by ships from North Vietnam on August 2, 1964. Two days later another attack was reported, but that report was based on misinterpretation of radar imagery - an error that was quickly

[13] Allen Whiting, *China Crosses the Yalu* (NY: Macmillan, 1960).
[14] Yee, Herbert S. 1980. "The Sino-Vietnamese Border War: China's Motives, Calculations and Strategies." *China Report*, Jan.-Feb. 1980. Pp. 15-32.
[15] Allen S. Whiting, 2001, "China's Use of Force, 1950-96, and Taiwan," *International Security*, Vol. 26, No. 2 (Autumn, 2001), pp. 103-131.
[16] Adapted Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use" in Proceedings of a Workshop on Deterring CyberAttacks, Committee on Deterring Cyberattacks, National Research Council. 2010.
http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_059437.pdf

identified but not corrected until much later.[17] In any case, only three days after the second "incident" Congress passed of the Gulf of Tonkin Resolution that provided justification for Presidential action for the rest of Vietnamese War. The lesson for the cyber realm is that evidence of an attack needs to be verified with care.

17. The Cold War

Implication: The lesson most Americans have derived from the Cold War is that a patient policy of containment was successful. The implication of invoking the Cold War is that rivalry can be limited and crises need not explode.[18]

18. Mutual Assured Destruction

Implication: Deterrence of nuclear war, and even direct combat between the superpowers, was (apparently) effective for sixty years, making deterrence a highly salient concept for the prevention of cyber war. Despite the attempts to adapt the concept of deterrence to the differences between kinetic and cyber conflict, it has been a stretch. For example, the core concept of mutual assured destruction does not apply. Likewise, the core concept of deterrence that requires clarity of response in order to achieve credibility of commitment does not necessarily apply to cyber conflict since ambiguity might be helpful to avoid retaliation, even if the ambiguity lessens deterrence. (For more on China's use of ambiguity, see analogy 24, "Chinese Restriction of Rare Earth Exports," and the Appendix.)

19. Escalation Ladder

Implication: The clarity of the nuclear threshold has helped sustain the taboo against the use of nuclear weapons. There are potential thresholds between cyber espionage and cyberwar, but they are not yet widely understood or agreed upon. Nor is there even convergence on how the terms should be defined. There is not even convergence on what kinetic actions in response to a given kind of cyber attack would constitute escalation or de-escalation.

20. Control of Chemical Weapons

Implication: Even without effective verification, agreements on limiting cyber attacks (e.g. to military targets) could prove effective.

21. MIRV (multiple independently targetable re-entry vehicle)

Implication: In a rivalry, the side with a technical advantage (such as the U.S. had in the 1970s with MIRVs) may miss an opportunity to prohibit a destabilizing technology. In the case of MIRVs, detection is easy at the stage of testing, but almost impossible once deployed. In retrospect, the U.S. would have been better off with an early arms control treaty banning the testing of this destabilizing technology. At the time,

[17] Robert Hanyok, 1998. "Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2-4 August 1964, *Cryptologic Quarterly*. The declassified version of this report by the NSA Historian is available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB132/relea00012.pdf

[18] For other analogies from the Cold War, see Sulek, David and Ned Moran. 2009. "What Analogies Can Tell Us About the Future of Cybersecurity." Pp. 118-131 in *The Virtual Battlefield: Perspectives on Cyber Warfare*, vol. 3, *Cryptology and Information Security Series*, edited by C. Czosseck and K. Geers. Amsterdam: IOS Press.

however, the well-established principle prevailed that a military advantage should never be voluntarily surrendered, and there was little or no consideration of the destabilizing potential of that technology. The analogy will be apt when one side has a lead in a technology that would be destabilizing if deployed by both sides of a rivalry, and whose prohibition would be more reliably verifiable before deployment than afterwards.

22. 9/11

Implication: There are terrorists who are plotting to do maximum damage to the U.S. population. Beside the obvious possibility of nuclear or biological weapons, there is also the potential danger of a cyber attack on a critical target such as a dam, hospital, power grid, or water purification system.

23. Wikileaks

Implication: When classified information is widely distributed to promote the "connection of the dots", there is a corresponding risk of massive leakage.

24. Chinese Restriction of Rare Earth Exports

Implication: An act by one country that harms another is often ambiguous in its intent, even if the effect and the perpetrator are both clear. On September 7, 2010 the Japanese detained the captain of a boat in waters around a disputed island. The Chinese then cut their exports of rare earths by 72%. Since rare earths are essential for a variety of electronic and other industrial products, and China controlled 95% the global supply, the timing of the export restriction was seen by many in Japan and the West as retaliation, despite Chinese denials.[19] For more on the Chinese tactic of denying retaliatory intent, see the Appendix.

25. Cyber Espionage

Implication: Espionage is done by everyone and is not an act of war. Nations maintain a "polite fiction" that they don't do it, even if their rivals do. The burden is on the defense. Revealing espionage often harms bilateral relations. The amount of harm done by cyber espionage, especially by China, is substantial but the U.S. public has not been aroused in part because proof of the source and the extent are not publically available.

26. Cyber Attack on Siberian Pipeline

Implication: Cyber industrial sabotage by means of malware is nothing new. In 1982, the CIA introduced a logic bomb into exported pipeline software that was picked up by the KGB, leading to "the most monumental non-nuclear explosion and fire ever seen from space."[20]

[19] "China Denies Japan Rare-Earth Ban Amid Diplomatic Row," *Bloomberg News*, September 23, 2010.
[20] Reed, Thomas C. "At the Abyss: An Insider's History of the Cold War," (New York: Ballantine Books, 2004). See also sources cited in the Wikipedia article on "Siberian pipeline sabotage".

27. Cyber Attacks on the Iranian Nuclear Program

Implication: The use of cyber attacks by the U.S. and Israel against infrastructure (as opposed to cyber espionage) now has a precedent,[21] making it easier for other nations to justify another such attack. A potential "red line" still exists for attack on financial systems.

28. DigiNotar Certificate Authority Breach

Implication: Even the most trusted category of cyber authority could have "shocking ineptness" in its security system. DigiNotar was a supplier of trusted certificates to authenticate that a request on the internet was being sent to the intended party. In 2011, over 500 false certificates for domains such as Google and Yahoo were issued through DigiNotar by an Iranian hacker. This hack resulted in 600,000 requests that were subject to a "man-in-the middle" attack. Over 95% of these requests came from Iran, suggesting that the purpose was to spy on Iranian internet users. After the fact, an audit showed that DigiNotar's

> servers ran out-of-date software. Its network was poorly segmented, so problems would not be contained if they arose. Passwords in play at the time of the hack might easily have been guessed via brute-force attack. In addition, there was no secure logging and server-side anti-virus protection was absent.[22]

In my opinion, some or all of these failures in elementary security practices would have been known and must have been tolerated by co-workers. The most important lesson is that cyber security indoctrination should include a version of West Point's Honor Code such as "I will not violate cyber security procedures, or tolerate those who do."[23]

D. Functional Analogies

29. Biodiversity vs. Weakest Link

Implication: The biodiversity metaphor suggests that diversity of cyber systems may result in resilience against attacks. On the other hand, if the problem is to protect information stored in various systems, the "weakest link" metaphor suggests that diversity of cyber systems makes the defense as weak as its weakest component.

30. Herd Immunity

---

[21] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012.

[22] John Leyden, 2011. "Inside 'Operation Black Tulip': DigiNotar hack analysed" *The Register*. http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/
See also Fox-IT (August 2012). *Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach.*

[23] What is needed is a metanorm, i.e., a norm against tolerance of norm violations. See Robert Axelrod, 1986. "An Evolutionary Approach to Norms," *American Political Science Review*, vol. 80, pp. 1095-1111. http://www-personal.umich.edu/~axe/Axelrod%20Norms%20APSR%201986%20(2).pdf

Implication: If a sufficient proportion of the population is immune to a disease, the disease is unable to spread among the vulnerable parts of the population.

31. Crime

Implication: A wide range of private (as opposed to state-sponsored) cyber activity can be suppressed by ordinary police work and the criminal justice system.

32. Child Pornography

Implication: Some things are universally abhorred, and such things could be the basis of initial understandings and norms about activities in cyber space.

33. Territorial Responsibility

Implication: The legal principal that a state is responsible for the prevention of illegal acts emanating from its territory can be extended to cyber space to hold nations responsible for cyber activity launched from its own territory. While the origin of a cyber activity is often impossible to trace, there may be times when its origin can be established.

34. World Trade Organization

Implication: The principle of equivalent retaliation built into the treaty of the World Trade Organization makes enforcement of its rulings quite effective. If such a principle could be established for violations of norms in the cyber world, self-help enforcement could also be effective.

35. Insurance and Industry Standards

Implication: Individuals and companies purchase insurance to mitigate the effects of theft and other crimes. In turn, insurance companies often set standards that require certain anti-theft measures to reduce their liability. Insurance against cyber crime is not a well-established industry, largely because of the difficulty of assessing damage from a cyber crime in monetary terms. Nevertheless, there may be value is exploring whether the standards required by insurance companies could be adapted to prevent cyber crime. For example, the computer security industry could set standards and issue the equivalent to a "Good Housekeeping Seal of Approval" to companies that meet those standards.

Appendix
Chinese Tactic of Denying Retaliation

The historical analogy number 24, "Chinese Restriction of Rare Earths Exports" is worthy of elaboration because it involves an unusual tactic that China has used several times recently, and is readily adaptable to cyber conflict.

In the last two years, China has employed a new pressure tactic against three countries with which it has a dispute: Japan, North Korea, and the Philippines. In each

case, China suspended trade in specific commodities, while refusing to acknowledge that the trade suspension had anything to do with the dispute. In two of the cases, China has apparently achieved its immediate goals, and the third case is still unfolding.

* After a Chinese ship captain was detained in Japan for sailing in waters near a disputed island on September 7, 2010, China drastically curtailed its exports of rare earths. Rare earths are important in the manufacture of many electronic products, and China controlled 95% of the global supply.[24] China denied it had a trade embargo with Japan, but after the captain was released, the trade returned to normal.[25]

* In January 2011, China suspended oil supplies to North Korea following the North's shelling of Yeonpyeong Island in what was widely interpreted as an effort to prevent Pyongyang from carrying out its threats to retaliate against the South if the South went ahead with its live fire exercises as planned.[26] China has not publically acknowledged its oil cut off, let alone provided a reason. Earlier suspensions without public acknowledgement have apparently occurred in 2003[27], 2006[28], and 2008[29]. For example, in March 2003, China suspended oil shipments to North Korea for three days due to "technical difficulties" soon after Pyongyang test-fired a missile into waters between Korea and Japan. The move was widely interpreted as a successful effort to get North Korea to attend a trilateral meeting in Beijing the following month.

* On April 10, 2012, a Philippine naval ship tried to arrest Chinese fishermen near a disputed reef in the South China Sea. China then refused to allow 150 containers of bananas to enter its market, saying that the bananas were "crawling with insects." The Philippines denied the charges and said that the insects the Chinese cited attack coconuts, not bananas.[30] China never acknowledged that its interruption of trade with the Philippines was linked to the territorial dispute.

Four questions arise with respect to these cases: what's new in the Chinese tactic, why deny, why China, and what's next?

What's New?

Countries have frequently resorted to economic pressure to get their way on some dispute. What is new in the Chinese tactic is the refusal to acknowledge that the pressure has any relationship to the issue at hand. I can think of no other country using a trade disruption to provide pressure on a security issue, where the timing of the disruption was publically presented as totally coincidental.

---

[24] http://www.bloomberg.com/news/2010-09-23/china-denies-japan-rare-earth-ban-amid-diplomatic-row-update1-.html

[25] http://online.wsj.com/article/SB10001424052702303879604577409831672468236.html

[26] http://www.koreatimes.co.kr/www/news/nation/2011/01/117_79966.html. Earlier suspensions of oil shipments to North Korea apparently took place in 2006 and 2008. http://www.nytimes.com/2006/10/30/world/asia/30iht-oil.3334398.html and nautilus.org/napsnet/napsnet-special-reports/dprk-prc-trade-aden/

[27] http://www.armscontrol.org/act/2009_07-08/zhang

[28] http://www.nytimes.com/2006/10/30/world/asia/30iht-oil.3334398.html?_r=1

[29] http://nautilus.org/napsnet/napsnet-special-reports/dprk-prc-trade-aden/

[30] http://www.csmonitor.com/World/terrorism-security/2012/0515/Philippines-feels-the-economic-cost-of-standing-up-to-China

Of course, other countries have often used economic pressure to attain security goals. For example, in the 1956 when Britain and France invaded Suez, the United States successfully used financial pressure to force them to withdraw. But the United States did not claim that its financial sanctions were merely coincidental. Nor has Pakistan claimed any pretext when it expressed its anger at U.S. actions by halting NATO supply trucks en route to Afghanistan in 2010 and again in 2011.[31]

There are also many cases in which a country took military action that it did not acknowledge, or even sought "plausible deniability." The U.S. responsibility for the Bay of Pigs invasion is just one of many examples, some successful and some not.[32] But I can't think of any incidents in which the actions in an economic domain were done to apply pressure in a security domain, along with claims that the timing of the economic pressure was purely coincidental.

In fact, standard strategic doctrine - as understood in the West - emphasizes that threats and warnings should be explicit for two reasons: to achieve maximum credibility, and to make clear what must be done to end the pressure. This raises the questions of why one might deliberately deny that a trade disruption is related to the security issue at hand, and why is China the one using this new tactic.

Why Deny?

Apparently the purpose of denying that the trade disruption is related to the security issue is to allow the other side to save face when backing down. Even if everyone knows that there is a linkage, the idea that there isn't any linkage is something we might call "a polite fiction."[33]

Polite fictions are common in everyday discourse such as the polite fiction "All teachers at our school admire one another and the principal." Everyone knows or suspects this is a fiction, but the statement's veracity is never pressed. It serves like the willing suspension of disbelief—allowing everyone to maintain the personae they have constructed for the purpose of social interaction.[34]

In blunt strategic terms, the polite fiction of the Chinese tactic of denying that undue pressure is being brought to bear lowers the cost to the other side of backing down - something of obvious value to the Chinese.[35]

---

[31] http://www.juancole.com/2010/10/pakistan-opens-khyber-crossing-to-nato-supply-trucks-but-issues-threats-over-hot-pursuit.html and http://articles.cnn.com/2011-11-27/asia/world_asia_pakistan-nato-attack_1_nato-helicopters-khyber-agency-nato-trucks?_s=PM:ASIA

[32] The Chinese certainly believe that the U.S. attack on their embassy in Belgrade on May 7, 1993 was an example of a deliberate attack that was presented to the world as a mistake. For evidence that it was deliberate see John Sweeney et al. "Nato bombed Chinese deliberately," *The Guardian/The Observer*, Oct. 16, 1999.
http://www.guardian.co.uk/world/1999/oct/17/balkans

[33] In the context of international relations, the concept of a "polite fiction" was apparently first used to describe the obviously false claim by the Soviets that they never engaged in spying. Robert Axelrod and William Zimmerman, "The Soviet Press on Soviet Foreign Policy: A Usually Reliable Source," *British Journal of Political Science, 11* (April 1981), pp. 183-200.

[34] http://www.justmusing.net/2010/01/26/polite-fiction/

[35] For a formal game theoretic model in which "saving face" is important, see Barry O'Neill, *Honor, Symbols and War*, 1999 (Ann Arbor, MI: University of Michigan Press).

Why China?

It is often said that East Asian cultures are more concerned with "saving face" than Western cultures are. Perhaps so, but there are plenty of examples in which Western countries have put great store in saving face.[36] For example, in the Cuban Missile Crisis President Kennedy took care to call his action a "quarantine" rather than a "blockade" because a blockade was an act of war and he did not want the Soviets to have to acknowledge giving in to an act of war. Even more important, in the deal that resolved the crisis, the Americans insisted to the Soviets that the promised removal of American missiles from Turkey would be kept secret so that neither the U.S. nor its Turkey ally would lose face when the missiles were actually removed a few months later.[37]

So if other countries have also been concerned with saving face, why has China been the one to invent the tactic of claiming that the timing of its economic pressure was only coincidentally related to a security issue? One reason is that China is concerned to support its claim that it seeks a "peaceful rise". For this reason it wants to avoid acknowledging that it uses undue pressure to resolve security issues. Another reason why China, rather than a Western power is the one to invent this tactic is that (as described earlier), ambiguous threats and warnings are simply inconsistent with the dominant Western conception of how to achieve deterrence and compellance. One might want to be a bit vague about the consequences if things escalate, but one wouldn't want to leave any unnecessary doubt in the target's mind that a threat was being issued, and one would want to display as much commitment as possible that further action would be taken if the situation remained unsatisfactory. Or so says standard Western security doctrine.

Indeed the Western approach to clarity draws not only on game theory, but also on major lessons from the outbreak of the two most traumatic events in the West, namely World War I and World War II. At the outbreak of World War I, Britain had not yet made clear that it would declare war on Germany if Germany violated the neutrality of Belgium. An important lesson was that clarity might have deterred Germany from invading Belgium.[38] Likewise, a major lesson from the failure to deter Germany from launching World War II is that the Allies should have decided much earlier and made it very clear that they would resist Hitler's aggressive demands by force if necessary. On the other hand, China's experience - both before and after 1949 - is that subtlety is often better than clarity.

What Next?

China's use of its new tactic has clearly achieved its immediate goal when applied to both Japan and North Korea, but it is too early to tell if it achieved its immediate goal

[36] For many examples, see Barry O'Neill, *Honor, Symbols and War*, 1999 (Ann Arbor, MI: University of Michigan Press), especially pp. 139-63.

[37] Israel also provides examples of not acknowledging its actions, even when there is no pretense of plausible deniability. For example, Israel has not acknowledged its possession of nuclear weapons, or its 2007 aerial attack on a Syrian nuclear facility. In both cases, an important goal is to allow other parties to avoid having to respond to Israel's actions.

[38] See for example Barbara Tuchman, *The Guns of August*, 1962 (NY: Macmillan)

when applied to the Philippines. But it is plausible to assume that the tactic works well at a low enough cost to China would be used again when the conditions are right. The conditions seem to be that China wishes to exert pressure in a given domain (such as a security issue), but wants to avoid the appearance of using pressure. The desire to avoid the appearance (or at least the acknowledgement) of pressure can be due to several factors including China's desire to maintain its posture of "peaceful rise," its desire to avoid domestic reactions from its own public or the publics of the targeted country, and its desire to make it easier for the other side to give in to China. No doubt these conditions are likely to arise many times in the years to come, not only on issues related to sovereignty over disputed islands, but on other issues of deep concern to China in dealing with countries like North Korea and perhaps Taiwan.

China must, however, weigh the prospects of short-term success with the possibility of long-term costs of its new tactic. For example, China's disruption of rare earth exports was quickly followed by Japan's release of the Chinese sea captain it held, but it also led to a global awareness of China's virtual monopoly of the supply of these valuable materials.[39] The result has been a buildup of inventories of rare earths and a readiness to restore production elsewhere, two steps that will soon dramatically reduce the vulnerability of other countries to any future disruption of Chinese exports of rare earths. In retrospect, China may regret not having saved its one-time opportunity to exert this pressure in a dispute of greater importance to China.[40] They may also come to regret having escalated pressure on the Philippines, the result of which may be greater U.S.-Philippines security cooperation - albeit under the polite fiction that it has nothing to do with China.[41]

In a future confrontation with the United States, a country might choose to use a cyber attack rather than an economic action. A cyber attack could be designed both to show displeasure with the United States, and to imply the possibility of escalation if it is not satisfied with the American response. A cyber attack has the advantage of not being as easily attributable as an economic action would be. To make it easier for the U.S. to give in, the instigator may once again assert that whatever harm occurred was not intended, and that the timing was purely coincidental.

[39] An interesting comparison with the Sino-Japanese territorial dispute is the Korean-Japanese territorial dispute. The latter has involved various forms of pressure but all have been directly related to the dispute rather than indirect or unacknowledged pressure in some other domain such as trade. See for example the sources in Wikipedia's "Liancourt Rocks dispute."

[40] On when to use a potentially fleeting resource in a rivalry, see Robert Axelrod, 1979. "The Rational Timing of Surprise," *World Politics 31*. pp. 228-246. http://www-personal.umich.edu/~axe/research/RatSurprise.pdf

[41] For example, earlier pressure from China let Secretary of State Hilary Clinton to say, "our long mutual defense treaty and alliance relationship with the Philippines [requires] working with the Philippines to provide greater support for external defense particularly maritime domain awareness, defensive ones, maritime boundaries." Williard Cheng, "Clinton Heaps Praise on Pacquiao, reaffirms US support for PH," ABS-CBN News, Nov. 11, 2011.