Calibrating the Cyber Warfare Threat Using Examples from Recent History

Matthew Cadbury (University of Hertfordshire)

Abstract

Cyberwarfare has emerged as a new mode of conflict. The level of threat posed by this new mode of conflict needs to be calibrated with other forms of warfare. Cyberwarfare has the capability to inflict enormous economic damage while rarely causing loss of life. This particular combination of effects makes it difficult to assess how seriously cyberwarfare should be treated, in particular whether it should be assessed at a lower level of threat equivalent to economic warfare or at a higher level of threat equivalent to conventional military action.

Errors in correctly calibrating threats have always been a feature of conflict. This paper examines four recent historical errors in assessing threats. While none of these historical examples is directly comparable to cyberwarfare, specific details and common themes between them might be helpful in assessing the new threat. The paper suggests that a combination of underestimated threats combined with vigilance to reduce exposure to them may be optimal and that it is important to avoid biases and emotional arguments when assessing threats. Applying these findings to cyberwarfare implies that cyberwarfare should be calibrated as a form of economic warfare and responses to cyber warfare should therefore be economic and political rather than military. This calibration should ideally be combined with steps to minimise the exposure of vital services to cyberattack and avoidance of bias in assessing the threat.

Introduction

The internet has enabled open communication between devices connected to it all over the world. The connecting of devices has also opened up the possibility of sending communications that contain damaging content and accessing devices to cause damage to them. Initially such cyberattacks were done mainly by individuals, but governments have increasingly taken an interest in the possibility of damaging other countries via its information technology systems as a form of warfare. The main attractions of cyberwarfare are threefold:

- Damage to information technology systems has the potential to cause extensive economic losses.
- Attacks rarely cause loss of life.

- It may be difficult for the target of a cyberattack to prove who was to blame, especially as a cyberattack and the damage it causes may occur at different times.

An attacker thus has the ability to cause considerable damage without physical violence and without admitting responsibility. As the activities of a nation are increasingly linked together via the internet, the extent of the potential to cause damage through cyberwarfare increases; additionally, greater damage can be caused in more developed nations.

There is little public disclosure of the extent to which such attacks take place, even when the perpetrators are known. Two well-known examples are the US/Israeli Stuxnet software, which was used to cause malfunctions to uranium centrifuges in Iran, and North Korea's WannaCry virus, which attacked a weakness in Microsoft Windows to encrypt files. It is clear that cyberattacks can cause extensive damage. The WannaCry virus was estimated to have caused $4 billion in damage (Fulford, 2017), and there is the possibility that far more extensive damage could result from a more ambitious attack: "a string of such attacks on, for example, the American power generation grid could threaten the very survival of the nation." (Helms 2015) To date there is limited experience of attacks of such magnitude, and it is difficult to predict how serious cyberwarfare might eventually prove to be. It is this uncertainty which makes it difficult to calibrate the threat of cyberwarfare compared with other forms of hostilities.

Threats need to be accurately calibrated for adequate preparation to be made and appropriate responses taken. This paper considers four examples from recent history in which threats were wrongly calibrated: Chamberlain at Munich in 1938, the German response to evidence of the breaking of the Enigma code in 1942, the Arab/Israeli war of 1967, and the Iraq war of 2003. None of these examples is directly comparable with cyberwarfare, or with each other, but their complexities and circumstances shared cyberwarfare's inherent difficult in calibrating the threat. This rendered them in some way analogous to the difficulty of assessing today's threat of cyberwarfare and suggests the possibility of learning lessons from them for cyberwarfare.

Munich 1938

The peace treaties that ended World War I imposed on Germany a series of ongoing military limitations and stripped Germany and Austria-Hungary of significant territories where the majority of the inhabitants were ethnic Germans. Even at the time, this was widely regarded as unjust, including among representatives of the victorious Allied powers.

In 1938 the German Government under Adolf Hitler demanded the cession of the "Sudetenland" in northern and western Czechoslovakia (home to a majority German population) to Germany. A meeting was arranged in Munich to discuss this demand and Britain's Prime Minister, Neville Chamberlain, took the lead in the negotiations. An agreement was reached that Germany could have the Sudetenland on condition that Germany would make no further territorial demands. Chamberlain believed that he had defused a serious crisis and, infamously as it turned out, described the agreement as "peace in our time" (Chamberlain, 1938). Chamberlain was nevertheless wise enough to take precautions, and while Britain's armaments production trailed Germany's at the time of Munich, it was rapidly catching up. It became clear that Chamberlain had misjudged the situation when Germany occupied the whole of Czechoslovakia a few months later.

With the benefit of hindsight, it seems obvious that the Munich agreement was not only a mistake, but a mistake so obvious that Chamberlain's policy has given the word "appeasement" a derogatory connotation. Yet at the same time, the potential consequences of any action that might provoke war were very serious for the underprepared West. The number of military casualties in World War I had shocked the world, and there was both preliminary evidence and a general expectation of high civilian casualties from bombing or gassing in any future war. By comparison, the return of the Sudetenland seemed a modest sacrifice. The Munich agreement was criticised by some at the time, notably Winston Churchill, but was for the most part received with relief and Churchill himself acknowledged that "Neville Chamberlain acted with perfect sincerity" (Churchill, 1940). Chamberlain had underestimated the threat that Hitler posed, but did implement countermeasures that would contribute significantly to Britain's survival when the threat materialized and Britain came under German attack less than two years later.

Enigma 1942

The Enigma machine was an enhancement of a commercial encryption system that the German military used for radio transmissions. Radio transmissions could be easily intercepted, and thus achieving secrecy relied on encryption of the messages transmitted. The machine worked by transforming each letter in the source text into a different letter. Inside the machine were rotor wheels which moved each time a letter was transformed, such that the basis of transforming the next letter was different from the previous one. The method of encryption was thus a moving target. To provide an added layer of security, the settings of the rotors were changed each day. Germany's military believed the system could not be broken and, given that belief, routinely sent highly confidential information by radio.

Germany's confidence in the Enigma machine turned out to be misplaced. Rudimentary automated systems were able to decrypt some messages, and ultimately the world's first computer was developed for the task. Breaking the Enigma code was never easy and, because of the daily change in settings, Enigma essentially had to be broken anew each day. There were days when Enigma was broken, and a significant number of messages decrypted, and days when it was not broken and no messages decrypted.

It was essential that Britain keep decryption secret, and only a handful of senior military, politicians and civil servants were informed. However, there was also the risk that German commanders might guess that their secrets had been discovered if Britain took action too obviously on the information received. One such situation arose in 1942 when Enigma decrypts were used to locate German submarines in the Atlantic. Germany's Admiral Karl Dönitz was suspicious that communications with his submarine fleet might have been monitored (Hastings, 2015). The German navy did update its Enigma machines with an additional rotor wheel at this point, and it took some time before the British could break the German naval code again. Nevertheless, the overall integrity of the Enigma system was not questioned, and other branches of the German military took no action.

In hindsight, it seems obvious that the Germans should have realised there was a problem with Enigma. But a confounding factor for Dönitz was the comparative ease with which German naval intelligence was able to break the codes used for British convoy radio communications. If Britain could not properly encrypt its own radio signals, then why should he have believed it possible that Britain could be decrypting Germany's more advanced system? The British incompetence in encryption may thus have contributed to saving their decryption success from detection (Hastings, 2015). A further problem for Germany was that Enigma was used across all its command systems. To change or replace Enigma would have required resources and caused disruption, which Germany's already stretched military could ill afford. Germany had underestimated the threat to Enigma and took little action to mitigate the threat.

Israel 1967

When Britain withdrew from Palestine in 1948, the Jewish community was attacked by its Arab neighbours, but defended itself and formed the state of Israel. Tensions continued along Israel's borders and, in response to fighting between Syria and Israel in the Golan Heights in 1967, Egypt moved forces toward Israel's southern border. To Israeli intelligence, it seemed likely that an attack on Israel was imminent. Israel had recently equipped its air force with modern French Mirage jets, giving it the chance to seize control of the air if the opposing air

forces could be neutralized by a pre-emptive strike. This plan was put into effect with stunning results and within six days Israel controlled all of former Palestine.

In hindsight, it seems that Israeli intelligence had not fully understood the situation. Egypt was indeed moving forces towards the border; however, this was most likely in order to make a show of support for its Syrian ally rather than launch an attack. From Israel's perspective, the situation was made exceptionally difficult by geography. In 1967 Israel was only some twenty miles wide at its narrowest point, a factor which made it unwise for Israel to risk allowing itself to be attacked. This factor alone accounted for the Israeli decision to make a pre-emptive strike. Egypt's forces were taken completely by surprise when Israel attacked, a posture consistent with them not being in readiness to make an attack themselves.

Iraq 2003

In 1990 Iraqi forces had overrun Kuwait and were subsequently driven out by a coalition of Arab and Western forces. After this war sanctions were imposed and the Iraqi government agreed to disarm under United Nations supervision. A key aspect of the disarmament was to be the destruction of Iraq's chemical weapons arsenal. The UN disarmament program was highly effective and destroyed most of Iraq's weaponry, but there was disagreement over the quantity of Iraq's chemical weapons. The UN's calculations indicated that Iraq still had possession of approximately 10,000 gas shells. The Iraqi government denied possessing any more chemical weapons and suggested that these shells might have been lost in the previous war. UN inspectors searched a large number of likely sites, finding no evidence of chemical weapons. The USA decided to cut short the UN inspections, however, and went to war with the help of Britain and other coalition allies.

Despite some heavy street fighting in Nasiriyah (Pritchard, 2006), for the most part the Iraqi army drifted away. The invading forces soon captured Baghdad, bringing to an end all organized resistance and eliminating the authority of the Iraqi Government. The coalition officially disbanded the Iraqi army and removed all members of the ruling Ba'ath Party from public office. Unfortunately, the coalition focused principally on political objectives and lacked the manpower to impose military authority over all the territory it had captured. The rest of the country was left without any effective governance in the presence of over a million unemployed Iraqi soldiers and some 200 unguarded weapons stores. The result was anarchy. A new constitution worsened the situation by creating a centralized democratic government that gave the majority Shia population predominant power. The response of the minority Sunnis, who had previously dominated the government, was full scale rebellion. The chaos inside Iraq was not the only problem. Neighbouring Iran gained a significant regional role and intervened

heavily in Iraqi politics, where Shia militias asserted increasing power. The Kurdish regions of Iraq exercised autonomy and threatened to destabilize Syria and Turkey. Al Qaeda and other terrorist organisations, eventually including ISIS, thrived in the power vacuum.

In hindsight, it is clear that the rationale for invading Iraq was flawed – the missing chemical weapons were never found. It is equally clear that it was not sensible to launch an invasion with insufficient manpower to occupy the country. Nevertheless, it was difficult for the USA and Britain to assess the seriousness of Iraq's chemical weapons arsenal, and neither the UN nor anyone else could account reliably for the missing weapons. Saddam Hussein's regime also fuelled suspicion by denying UN weapons inspectors access to significant government sites. Chemical weapons, moreover, pose little threat to well-equipped military forces. A further challenge facing the USA in assessing the threat was the terrorist attacks of September 11, 2001, which not unreasonably pushed US strategic thinking towards pre-emptive strikes against possible future threats. There was also a moral rationale because the Iraqi regime had a long track record of brutality towards its own people, brutality that émigré Iraqi activists touted to an already receptive Western leadership. Some Western leaders were almost certainly aware that the objective military reasons for launching an invasion of Iraq were rather weak, but they believed that invading Iraq would bring freedom to the Iraqi people, would deter other nations from using chemical weapons, would bring long term regional benefits, and, likely, would deliver access to Iraqi oil fields.

Discussion

The Prussian military philosopher Carl von Clausewitz pointed out that war is an extension of politics by other means (Clausewitz, 1832), and that there is clearly a scale of seriousness of conflict between nations ranging from the political to the economic to the military. In our own age, this had been extended to nuclear conflict and conflicts potentially involving other weapons of mass destruction. Each successive level of conflict has greatly higher costs than the previous one. In general, a country facing an external threat would want to avoid unnecessarily causing conflict or escalating the level of conflict. This would suggest that, all things being equal, it is better to under-calibrate than over-calibrate threats.

In the above examples, security threats were under-calibrated in Munich 1938 and Enigma 1942. The obvious difficulty with under-calibration is that a country may make itself vulnerable by not taking immediate action against the threat. A key issue when underestimating a threat is thus the degree to which further steps are taken to mitigate that vulnerability. After Munich, Chamberlain presented a public position that war had been averted. Chamberlain's government had already authorized increased military expenditure and implemented a long-

term program to increase armaments production through "shadow factories" that could be activated if the international situation deteriorated further. By the time Britain faced direct attack in 1940, it was out-producing Germany in fighter aircraft by more than two to one (Holland, 2015) and was able to successfully defend itself. While Britain had underestimated the threat posed by Hitler, it had taken steps to counter it. Clearly vigilance in countering a threat is preferable to complacency, and Chamberlain's performance at Munich was better than it looks in hindsight. In the Enigma example, Germany continued to use Enigma despite mounting evidence that the system was compromised, including finding Enigma decrypts in mail bags on a captured merchant ship in May 1942 (Hastings, 2015). But here, too, the German assumption that the British were too unsophisticated to mask their own codes from decryption led them to believe that their own codes were at least generally speaking invulnerable. This under-calibration fatally led to a situation in which virtually all German messages sent after late 1942 were decrypted and read by the Allies and then exploited for military advantage. German officers debriefed after the war were shocked by the extent to which their signals were compromised, while Allied officers during the war were constrained to use German intercepts selectively enough to prevent the Germans from deducing the extent of their penetration.

In the examples of Israel in 1967 and Iraq in 2003, enemy threats were over-calibrated, resulting in wars that might not otherwise have taken place. The immediate consequence of Israel's pre-emptive strike was a brilliant military success that has, however, not worked in Israel's favour. Captured land could have been used as a bargaining chip to achieve a lasting peace, as the return of Sinai to Egypt proved to be in after 1978. Once in possession of the land, however, the temptation was to keep some of it for security purposes. Israel thus gradually created what George W. Bush would subsequently call "facts on the ground" through the establishment of settlements that further displaced Palestinians civilians, many of whom became radicalized and won a fair amount of world opinion to their cause, and that also gave Israeli radicals new homes and new soil to defend as their own. Israel's trump card of exchanging occupied land for peace has become increasingly difficult to play, and Israel remains locked in conflict with the Palestinian people. The Iraq war, after initial success, quickly became a disaster for the occupation, and even more so for hundreds of thousands of Iraqis. There was both an error in calibrating the risk faced and a high level of complacency in the planning and execution of the military strategy that was chosen. Even allowing for the difficult issues of assessing the risk of chemical weapons and the level of anxiety after September 11, 2001, the assessment of the Iraqi threat was poorly carried out. The UN had completed some 500 failed inspections (Arms Control Association, 2003), more than enough

to ring alarm bells both over the likelihood that chemical weapons truly existed and over the quality of US intelligence. Over-calibration of threats in these cases has been costly, especially when accompanied by complacency.

In the cases of Munich, Enigma, and Israel the threat seems to have been analysed and a decision taken without any obvious bias. The same could not be said for Iraq, where strategic analysis occurred with a strong background bias militating toward war. There is a perception that leaders of the USA and Britain lied about chemical weapons, but this is not a correct diagnosis of what happened. At the time almost everyone, including UN weapons inspectors, believed that Iraq possessed chemical weapons and there was genuine surprise that no chemical weapons were subsequently found. The dishonesty in the Iraq war of 2003 concerned the way that chemical weapons were portrayed through the use of the phrase "weapons of mass destruction" to blur the boundary between chemical and nuclear weapons. In the United States politicians went even further and overtly used the imagery of nuclear weapons, for example the expression "waiting for the mushroom cloud" (Kristensen, 2006). The supposed threat of Iraq's suspected chemical weapons were thus calibrated on a level closer to nuclear weapons than to conventional weapons. This was absurd, for the weapons that Iraq was thought to possess were short range battlefield weapons that posed a negligible threat to the USA and Britain. It is possible that US and British leaderships simply got carried away by their own rhetoric, or were simply ignorant of Middle Eastern affairs, but the consistency and extent of the exaggeration of the Iraq threat suggests that it was deliberate.

Conclusion

The above case studies suggested three general findings when calibrating threats. First, given the undesirability of provoking or escalating conflicts, threats should preferably be under-calibrated rather than over-calibrated. Second, the assessment of threats needs to be made as far as possible without bias. Third, it is better to be vigilant than complacent.

The first finding suggests that cyber warfare should be calibrated as a type of economic warfare. Responses to cyberwarfare should therefore be limited to political and economic actions rather than military action.

The second finding is that bias should be avoided. The case of Iraq showed the danger of emotive language being used to exaggerate the threat of chemical weapons. Leaders did not lie about "weapons of mass destruction;" the lie was "weapons of mass destruction," a phrase which created confusion between chemical and nuclear weapons. Both chemical weapons and

cyberwarfare are relatively new forms of conflict and thus open to the same kind of emotional manipulation. There is therefore a direct lesson from Iraq that new threats are open to exaggeration and this should be avoided in calibrating the threat of cyberwarfare.

Third, it is clear that vigilance in the face of threats is a better approach than complacency. Just as chemical weapons are very effective against unprepared targets and ineffective against well-equipped military forces, cyber warfare is also most effective when the target is weekly prepared. Failure to be vigilant against cyberattack was illustrated by the damage sustained by Britain's National Health Service from the WannaCry virus, where software updates had not been applied to many computers (Fulford, 2017). The threat we face from cyberwarfare also has similarities to Germany's problem with Enigma, in that in both cases important information is communicated openly. In the Enigma case the information was protected by encryption and today's information on the Internet is protected by software. Germany's error was to assume that encryption could be made 100% safe, and we would repeat that error if we assumed that software (which is often also encrypted) could be made 100% safe. In June 2017, the systems of the international shipping company Maersk were destroyed by the Russian NotPetya virus, but one complete set of national systems in Ghana was offline at the time due to a power cut and could be used afterwards to rebuild Maersk's global network (Greenburg, 2018). We should take steps to make software as safe as we can, but we should also take steps to keep some of the most vital services of the country offline, just in case.

References

Arms Control Association. (2003). *Disarming Saddam – A Chronology of Iraq and UN Weapons Inspections*. Washington, DC: Arms Control Association.

Chamberlain, N. (1938). Chamberlain's Speech on Sept. 30, 1938. http://news.bbc.co.uk/onthisday/hi/dates/stories/september/30/newsid_3115000/3115 76.stm.

Churchill, W. (1940). Churchill's Speech to the House of Commons, Nov. 12, 1940. https://winstonchurchill.org/resources/speeches/1940-the-finest-hour/neville chamberlain/.

Clausewitz, C. (1832). *On War*. New Jersey: Princeton University Press.

Fulford, M. (2017). *4 of the Most Expensive Cyber Attacks of 2017*. LBMC Information Security. http://www.lbmcinformationsecurity.com/blog/4-of-the-most-expensive-cyber-attacks-of-2017-and-how-they-could-have-been-prevented.

Greenburg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired.com. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hastings. M. (2015). *The Secret War*. London: William Collins.

Helms, C. (2015). *The Digital GCC: USCYBERCOM as a Combat Command*. Defense Technical Information Centre. http://www.dtic.mil/dtic/tr/fulltext/u2/1012758.pdf.

Holland, J. (2015). *The War in the West. Germany Ascendant 1939-1941*. London: Penguin Random House UK.

Kristensen. H. (2006). *Global Strike. A Chronology of the Pentagon's New Offensive Strike Plan*. Washington, DC: Federation of American Scientists.

Pritchard, T. (2006). *Ambush Alley: The Most Extraordinary Battle of the Iraq War*. New York: Presidio Press.