China’s ‘Cyberwar’ Against the US: Truth or Fiction?

1. Introduction.

On the 6th May, 2013, an Annual Report to Congress prepared by the Office of the Secretary of Defense claimed that in 2012 “numerous computer systems around the world, including those owned by the United States government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military”.1 This marked the first time cyberattacks on the United States were publicly attributed to the Chinese government by the American authorities.2 3 The report described Chinese cyberattacks as “a serious concern”,4 and certainly fear and speculation regarding China’s cyberactivity has been rife in both official and non-official circles for some years. Incidents of foreign network penetration and espionage seemingly conducted by the Chinese government have recently become both more frequent and more clearly attributable to the People’s Liberation Army (PLA) rather than independent nationalist hackers,5 and 33% of all cyberattacks in the third quarter of 2012 seemingly originated from China.6 For these reasons, while the Annual Report was careful to use qualifiers and to avoid sensationalist language, many commentators have played up the threat of China, often referring to China’s activities as ‘cyberwar’ against the U.S.7

---

2 Ibid.
4 Office of the Secretary of Defense, Annual Report to Congress, 36.
7 See for example: Magnus Hjortdal, ‘China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence’, Journal of Strategic Security 4:2 (2011); Alexander Abad-Santos,
word ‘war’ is sensationalist, emotive and brings to mind familiar forms of state-state interaction. In particular, it plays into wider media-driven narratives that, in the wake of the end of the Cold War and China’s rise to economic superpower, place China as the U.S.’s ‘natural’ adversary on the world stage. But is this ‘cyberwar’ truth, or a fiction? In order to ascertain the truth of the cyber-relationship between the U.S. and China, the term ‘cyberwar’ must first be defined, and China’s actions in cyberspace then examined with reference to this definition. By doing so, an assessment can be made regarding the nature of China’s actions and whether they truly constitute ‘cyberwar’.

2.1 The importance of defining ‘cyberwar’:

One serious problem is that there is no official definition of what constitutes ‘cyberwar’ either at the international level or at the domestic level in either China or the United States. This means that there is no single reference for judging whether or not a particular cyberattack meets the criteria for ‘cyberwarfare’. This lack of clarity is alarming when one considers that the U.S., for example, has stated its policy to respond to cyberattacks by any means appropriate within international law, including military action. Since international laws of warfare distinguish between actions that are permissible at times of war and at times of peace, then we must be able to consistently and accurately differentiate cyberwar from other aggressive forms of cyber activity and recognise incidents of cyberwarfare in order that we may respond lawfully in every eventuality.


9 Krekel, Capability of the PRC to Conduct Cyber Warfare and CNE, 19.

Given the high political and military sensitivity of state-on-state cyberattacks, it is vital that emotive terminology such as ‘war’ be used correctly. Should the Chinese find this use of language referring to their cyberactivities provocative, it has the potential to cause a diplomatic incident. Perhaps more importantly, casual use of the term ‘cyberwar’ in both official and non-official contexts may subconsciously encourage American policy-makers to view America’s cyber-relationship with China in an unnecessarily antagonistic light. Related to this, Lawson argues that use of the term ‘cyberwar’ has led policymakers to look primarily to war-related analogies to understand the cyber security situation. Yet ‘war’-related concepts such as ‘battlefield’ and ‘soldier’ have little useful meaning when applied to cyberspace, and analogies of cyberconflict as an echo of Cold War nuclear deterrence only serves to suggest that a fifty year-old strategy is the best solution to the new problems arising in cyberspace. For these reasons, if the term ‘cyberwar’ is to be used, it should be used sparingly and only when strictly appropriate with reference to established law about what constitutes ‘war’.

2.2 Broad definitions of ‘cyberwar’.

Jean-Loup Samaan divides commentators on cyberwarfare into alarmists, who claim cyberwar is present or imminent and who define it loosely, and sceptics, who adopt a narrower and more technical definition of ‘cyberwar’ (and indeed often take issue with the very concept of cyberwar itself). The alarmists largely follow ideologically from Arquilla and Ronfeldt, who defined ‘cyberwar’ in 1993 as conducting traditional military operations while destroying or damaging information and communication systems using cyber means. More recently Mehan adopted perhaps an even broader usage of ‘cyberwarfare’ adapted from Denning’s

warfare classification scheme: Class I cyberwarfare concerns low-level offensive
cyberactivities such as invasion of privacy; Class II industrial and economic
espionage; Class III any form of cyberattack carried out by any actor; and Class IV
the use of any cyber techniques in concert with kinetic military action.\(^\text{14}\) By allowing
any act by any actor (state, criminal or terrorist) to be considered ‘cyberwarfare’,
Mehan blurs the distinction between cyberwar, cybercrime and cyberterrorism. Yet
surely this should be maintained in the same way that ‘war’, ‘crime’ and ‘terrorism’
have distinct and largely mutually exclusive usages outside the cyber domain.
According to this definition, much of China’s cyberbehaviour can potentially be
defined as warfare – the Annual Report to Congress states that China’s activities
against the U.S. in cyberspace appear to be primarily focused on cyberespionage;
that is, the exfiltration of information from both U.S. government systems and the
networks of U.S. industries.\(^\text{15}\) Hjortdal\(^\text{16}\) and Ball\(^\text{17}\) consider the PLA’s use of
techniques such as network scanning and planting (dis)information mines to be
‘cyberwarfare’. However I argue that these definitions of cyberwarfare are unhelpful
due to the unspecificity of the term ‘war’ and their obscuration of real distinctions
between various types of offensive cyberactivity. A broad conception of
cyberwarfare should be rejected, and a more specific and technical description
sought with close reference to accepted definitions of the term ‘warfare’.

2.3 Narrow definitions of ‘cyberwar’.

Other definitions of ‘cyberwar’ have paid specific attention to existing
understandings of ‘war’, with reference to Carl von Clausewitz’s classic definition of
warfare and the laws of war under the Charter of the United Nations. Since the U.N
Charter was written long before cyberspace existed, however, there are no
international conventions specifically governing military conduct in cyberspace and

\(^{14}\) Julie E. Mehan, Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an
\(^{15}\) Office of the Secretary of Defense, Annual Report to Congress, 36.
\(^{16}\) Hjortdal, ‘China’s Use of Cyber Warfare’, 5.
it remains unclear whether the existing laws of war apply to cyberactivity or whether new legislation is required. As a result of this, attempts to apply the laws of armed conflict and Clausewitz's definition to cyberactivity have yielded some conflicting definitions.

Clausewitz's definition of war requires that any act of war be violent ("an act of force"), instrumental (acting "to compel the enemy to do our will") and political (war, as conceived by Clausewitz, is "a mere continuation of politics by other means"). Rid argues that no cyberattacks have yet met these three criteria (and that therefore there have not yet been any acts of cyberwarfare), and most have not even met one criterion. He ultimately concludes that all cyberattacks so far have simply been cyber-versions of espionage, sabotage or subversion, none of which should be considered as 'cyberwar' in their own right since each fails to meet all three of the criteria of an act of war. For example, cyberespionage (the most common cyberactivity perpetrated by the Chinese government upon American systems, according to the 2013 Annual Report to Congress) is rarely if ever violent; not usually instrumental (in that it aims not to achieve a goal in and of itself but simply to gather intelligence to aid the pursuit of a future goal); and not outwardly political, since it is intended rather by definition to be covert and therefore not politically attributed to any party. Outside of the cyber domain, espionage is not generally considered an act of war, and therefore it makes little sense to consider it one within the cyber domain. I agree with Rid, therefore, that Hjortdal and Mehan's inclusion of acts such as 'cyberespionage' in their conception of warfare is erroneous.

In trying to sculpt a definition of cyberwarfare that accords with Clausewitz's definition and the laws of war as set out in Article 2(4) of the U.N. Charter, there are

---

20 Ibid., 10.
21 Ibid., 6.
22 Office of the Secretary of Defense, Annual Report to Congress, 36.
23 Rid, Cyber War Will Not Take Place, 20.
four main areas of difficulty. The first concerns interpreting Clausewitz’s ‘act of force’ or the U.N.’s requirement of ‘armed force’ in a cyber context; the second is the difficulty of political attribution; the third the problematic nature of attempting to infer intention from cyberacts; and the fourth is the issue of whether or not cyberwar can take place independent of traditional war, and, if it cannot, whether it is meaningful to use the term ‘cyberwar’. These issues are examined below in the context of China’s cyberactivity.

2.4 Use of force and kinetic effect.

Both the Clausewitzian model and the U.N. laws require an act to be one of ‘force’ in order to count as warfare, implying the necessity of a kinetic effect – no act of war can take place that is entirely confined to cyberspace since at some point there must be actual or potential damage to the physical world.24 25 26 As McGraw succinctly puts it: “the means may be virtual but the impact should be physical”.27 This does not include attacks that do only financial damage,28 and the implications of damage to data are somewhat ambiguous because of differing domestic laws regarding its legal status, with the potential for misunderstandings between nations with different laws.29 Dinniss argues that, under international law, destruction of data alone might constitute an “unlawful interference” which invokes state responsibility for reparations but would fall short of ‘warfare’.30 This is because the physical damage caused by an attack needs to be more than de minimus, as well as being not too far removed from the chain of causation.31 Citing the incident whereby a computer virus called Stuxnet was (allegedly) used by the U.S. and Israel to destroy

24 Ibid., 6.
25 Dinniss, Cyber Warfare and the Laws of War.
27 Ibid., 112.
28 Dinniss, Cyber Warfare and the Laws of War, 41.
29 Ibid., 67.
30 Ibid., 73.
31 Ibid., 74.
centrifuges at an Iranian nuclear facility in 2010, she argues that while Stuxnet may have directly caused physical damage by speeding the centrifuges over their limit, it fails to meet the de minimus threshold for damage under Article 2(4).32

In cyberwarfare the ‘act of force’ may occur through a more complex and mediated process than in traditional warfare, due largely to the fact that the ‘weapon’ will be intangible. A hypothetical example of cyberwarfare supplied by Rid is that of a cyberattack which blacks out a city, resulting in (for example) train derailments and potential loss of life.33 Coincidentally the only Chinese cyberattacks to date that have been argued by some to meet the requirement of force involve the use of cyberattacks to effect blackouts. In 2003 two large-scale blackouts occurred in Florida and the U.S. Northeast.34 Harris’s detailing of the events makes clear his belief (despite official findings to the contrary) that Chinese hackers were behind the blackouts. Although no recorded damage was done as a result of either blackout, to fall under the Clausewitzian definition of ‘war’ the act must be only potentially lethal, and thus one could make the argument that a cyberattack on power grids constitutes an act of war. However in this instance there were no clear links to China, let alone the People’s Republic of China leadership, and the lack of any damage done would make it difficult to argue this as an act of war under Article 2(4).

Despite the lack of any publicly known Chinese cyberattacks amounting to actual uses of force, the consensus amongst commentators seems to be that the Chinese have the potential to perpetrate an attack of such a magnitude as to be considered ‘warfare’ under Article 2(4) of the U.N. Charter. The Annual Report to Congress expresses U.S. fears that, although no attacks have taken place that have caused significant damage or that can be linked definitively back to the Chinese government, the skills needed to conduct cyberespionage at the level the Chinese government is undoubtedly already carrying out could be employed to weaken or

32 Ibid., 81.
33 Rid, Cyber War Will Not Take Place, 9.
34 Harris, ‘China’s Cyber-Militia’.
damage the U.S. military in isolation or in combination with kinetic attacks.\textsuperscript{35} Also, should the Chinese have access to American power grids as Harris argues, then there is the potential for great damage to be wrought, but there is little evidence beyond speculation that the Chinese have ongoing access to key U.S. infrastructure, that they have attacked it, or that they have any specific plan to attack it.

2.5 Politicality and attribution.

Following Clausewitz’s definition, an act of force and the political intention behind it need to be attributed to an actor at some point during a confrontation for it to be considered an act of war.\textsuperscript{36} However this raises serious problems in cyberspace, where anonymity is easily maintained and most aggressive cyberacts are perpetrated covertly. Problems with attribution are common to all cyberattacks, but China’s cyberstrategy, as currently employed, has meant that conclusively attributing attacks on U.S. systems to the PRC leadership has been particularly difficult.

The first problem concerns the nature of cyberspace. Attributing an attack even to a geographic area is difficult, since attacks may be routed through servers in other countries, and in those cases where attacks can be reliably tracked back to an origin country it is nearly impossible to discover the identity of the individual at the computer behind the attack. This is particularly so in China, given the well-known weaknesses of China’s own networks - China in fact suffers the most attacks and viruses of any nation, which makes it an easy target through which to reroute attacks.\textsuperscript{37} The widespread use of botnets, whereby other peoples’ computers are infected and remotely controlled, often without their knowledge, causes additional difficulties in locating the source of an attack. Attacks that seem to be emanating from China are not necessarily being perpetrated by Chinese hackers.

\textsuperscript{35} Office of the Secretary of Defense, \textit{Annual Report to Congress}, 36.
\textsuperscript{36} Cited in Rid, \textit{Cyber War Will Not Take Place}, 8.
\textsuperscript{37} Hjortdal, ‘China’s Use of Cyber Warfare’, 12.
Secondly, while this applies somewhat to all nations, the Chinese government in particular has been reported to have deliberately adopted a strategy of decentralising the execution of cyberattacks in order to establish plausible deniability. Many Western commentators have reported that the Chinese government has recruited, trained and keeps a low level of control over a number of semi-independent “patriotic” hackers, whose loose affiliation with the PLA allows the PRC to claim credible deniability when they perpetrate an attack.\(^{38}\) Some elite hackers are inducted into PLA net militia units\(^{39}\) while others are, at a minimum, not discouraged from their nationalistic anti-American cyberactivity.\(^{40}\) This “military-civilian blurring” is continued in the PLA’s sponsorship of universities and institutes that support research and development in information warfare.\(^{41}\) In total Mazanec cites estimates of 50,000 military hackers either working or in training who will populate over 250 cyber units,\(^{42}\) although Stevens thinks this is an overestimation.\(^{43}\) Hjortdal meanwhile cites a leaked FBI report claiming that China had a “cyber army” of 30,000 military cyber spies and 150,000 private spies.\(^{44}\) Regardless of the number of semi-independent hackers, China is known to have divisions of the military devoted to cyberactivity, including the 3rd and 4th departments of the PLA General Staff\(^ {45}\) and Information Warfare units.\(^ {46}\) Some cyberattacks on U.S. networks have actually been traced with some reliability back to the Chinese military – for example, the U.S. cyber-security firm Mandiant reported that it had linked hundreds of attacks across various industries to a Chinese military hacking


\(^{40}\) Harris, ‘China’s Cyber-Militia’.

\(^{41}\) Hjortdal, ‘China’s Use of Cyber Warfare’, 11.

\(^{42}\) Mazanec, ‘The Art of (Cyber) War’.

\(^{43}\) Stevens, ‘Breaching Protocol’.

\(^{44}\) Hjortdal, ‘China’s Use of Cyber Warfare’, 10.

\(^{45}\) Ibid., 11.

\(^{46}\) Krekel, Capability of the PRC to Conduct Cyber Warfare and CNE, 33.
team known as Unit 61398 (BBC). Additionally, the industrial espionage operation labelled 'Operation Aurora' which aimed to steal source code and other intellectual property from several U.S. companies, including Google, was traced back by the cyber security company McAfee to a hacking group in Beijing with apparent ties to the PLA. However there is still no concrete evidence of the PLA’s direct involvement in any specific cyberattack.

The third, perhaps greatest problem is that to date China has denied involvement in any cyberattacks. This means that no cyberattack thus far meets the requirement of political intent, as laid out by Rid, since no certain attribution can be made of any attack to the Chinese government and there has been no declared political intent behind any attack.

2.6 Intentionality

When assessing whether or not a cyberattack constitutes an act of war, a further problem arises as to whether an attack should be judged with primary reference to its end result or its original intent. If one judges by outcome, then it is possible that an attack may have an unintended physical effect that raises it above the threshold of what constitutes ‘warfare’. On the other hand, attempting to judge by intention is perhaps even more problematic, relying as it does on the near impossibility of accurately divining the motivation of one’s adversary. This is rendered even more complicated in cyberspace due to the anonymity of its users and the problem of attribution.

With regard to China, there is very limited access in the West to materials (especially English-language materials) accurately reflecting the intentions of the PRC leadership. However several commentators find, based on available Chinese sources, that the primary motivations behind the PLA’s offensive actions in

---

48 Ball, ‘China’s Cyber Warfare Capabilities’, 89.
49 Dinniss, Cyber Warfare and the Laws of War, 55.
cyberspace are firstly espionage, both industrial and political,\(^{50}\) and secondly 
deterrence.\(^{51}\) (Given that China is also the victim of just as many attacks from other 
states, including the U.S., its apparent aggression may also be explained as active 
defence on China’s part.\(^{52}\)) Conducting cyberespionage to acquire industrial, 
political and military secrets does not constitute cyberwarfare per se, as discussed 
previously, and does not indicate any desire for immediate conflict (although 
gathering intelligence on the U.S. military would certainly benefit China in the event 
of any future conflict). China’s behaviour in cyberspace is likely influenced by its 
knowledge that it cannot hope at present to succeed in a traditional military war 
against the greater firepower of the United States. Following in the Chinese tradition 
of asymmetric warfare,\(^{53}\) its strategy has therefore been to turn instead to 
cyberspace where it might effectively deter the U.S. from interfering in its relations 
with Taiwan, gain technical superiority and, in the event of impending war, be able 
to deliver a devastating first strike that will cripple the United States’ military 
capabilities enough to level the playing field once traditional battle commences.\(^{54}\)

Few if any commentators suggest that China is deliberately trying to provoke the 
U.S. into a kinetic war at this time and China has little to gain and a lot to lose from 
starting a full-scale war with the U.S. in the near future. In the absence of access to 
many Chinese sources regarding their true intentions, it seems acceptable to assume 
that for now, any action by China that technically falls within the narrow definition 
of cyberwarfare will likely be unintentional.

### 2.7 The potential for independent cyberwar.

One thorny conceptual problem concerns the potential for cyberwar to exist 
‘independent’ of traditional warfare. McGraw argues that isolated incidents of

---

\(^{50}\) Hjortdal, ‘China’s Use of Cyber Warfare’, 1.


\(^{52}\) Hjortdal, ‘China’s Use of Cyber Warfare’, 1.

\(^{53}\) Ibid.

\(^{54}\) Mazanec, ‘The Art of (Cyber) War’.
‘cyberwar’ have occurred using ‘cyberweapons’ such as the Stuxnet virus.\textsuperscript{55} To date, no such cyberattacks have triggered military conflict. However there is the potential for a politically attributed cyberattack to cause damage significant enough that it registers as an ‘act of war’ under international law, and to spark off full-scale military conflict.\textsuperscript{56} For such an attack to start a war that only takes place in cyberspace is regarded as less believable. Samaan makes a conceptual distinction between the terms ‘cyberattack’ and ‘cyberwar’ and states that while cyberattacks may have taken place, cyberwar has not and never will, since he argues that cyberattacks “are specifically not autonomous cyber-warfare”.\textsuperscript{57} Given that he draws the distinction and because it is highly unlikely that in the event of a cyberattack serious enough to meet the requirements of Article 2(4) there would be only a cyber, rather than a military response, he concludes that the whole notion of ‘cyberwar’ is “sci-fi”.\textsuperscript{58} However my conceptualisation of cyberwar is not as narrow as this, and I argue that individual acts may constitute acts of cyberwarfare if they fit Clausewitz’s definition and the laws of war. Indeed the PRC leadership also does not view cyberwarfare as an autonomous field of war, instead conceiving of it as a supplement to traditional military campaigns. Should China commit an intentional act of cyberwarfare, PLA strategy suggests that it would be employed as a pre-emptive strike before commencement of traditional kinetic warfare.\textsuperscript{59}

3 Conclusion

There is no official definition of what constitutes ‘cyberwar’, meaning that at present arguments can be made in support of wildly differing definitions. However I argue above that loose or broad definitions of what constitutes cyberwarfare create unnecessary and potentially dangerous confusion, limiting the ability of policy-makers to recognise and respond responsibly to different cyberthreats. I advocate

\textsuperscript{55} McGraw, ‘Cyber War is Inevitable’, 114.
\textsuperscript{56} Dinniss, \textit{Cyber Warfare and the Laws of War}, 130.
\textsuperscript{57} Samaan, ‘Cyber Command’, 16.
\textsuperscript{58} Ibid., 20.
\textsuperscript{59} Ibid.
instead for adopting a tight, technical and specific definition of ‘cyberwar’ drawing on Clausewitz’s classic construction and the United Nations Charter. Any cyberattack must itself cause physical damage in a reasonably direct manner, it must be instrumental, be politically attributable to the Chinese government and have occurred with their intent in order for it to be considered an act of cyberwar. Cleaving to this definition, China’s cyberbehaviour thus far falls short of constituting cyberwarfare, primarily due to the non-violent nature of its cyberactivity. Labelling all China’s offensive cyberactivity using the emotive term of ‘cyberwar’ can only worsen diplomatic relations between China and the U.S. by confusing the discourse, and conflating cyberwar with cybercrime and cyberterrorism results in “a dearth of effective policy dealing with any of the three”.60

It is likely that the Chinese government has conducted several cyberattacks in the past and that it will continue with that strategy.61 Chinese attacks against U.S. industries seem to be increasing, but are still focused on espionage rather than causing damage.62 It is likely, however, that China possesses the capabilities to conduct cyberattacks on the level of cyberwarfare,63 and some commentators warn that since much U.S. infrastructure is privately owned, Chinese espionage and attacks on private industry pose a potential danger.64 Yet, in comparison to the U.S., China’s cybercapabilities are still fairly rudimentary and Ball concludes that while a pre-emptive cyberstrike might be effective, China would have little chance of success in a full-out cyberwar.65 The PLA have demonstrated that they realise any cyberattack launched by a state and causing large-scale physical damage will be considered the start of an armed conflict,66 and it is highly unlikely that China will (intentionally) take that risk in the near future.

The term ‘cyberwar’ should be used sparingly, however, in order that, should such an attack occur, it might be clearly recognised and correctly responded to as

---

60 McGraw, ‘Cyber War is Inevitable’, 110-111.
63 Stevens, ‘Breaching Protocol’.
64 Harris, ‘China’s Cyber-Militia’.
65 Ball, ‘China’s Cyber Warfare Capabilities’, 101-102.
such. In conclusion, China’s cyberwar against the U.S. currently constitutes a fiction, but there is potential for it to develop into truth.