Is remote control effective in solving security problems?

Is Democratic Peace Theory Undermined on the Cyber Battlefield?

Archie Jobson

Abstract:

I have sought to answer this question from the perspective of international relations theory, more specifically democratic peace theory. In this essay I forward the case that the developments of cyber warfare negate the factors that promote the notion of democratic peace. These being the transparency of democracies, public aversion to the casualties and costs of war as well as the war retardant of free trade. This is significant for two reasons. Firstly, since the collapse of the Soviet Union the US, and its allies, have orientated their foreign policy around the promotion of democratic norms and governments. This could now mean a drastic change in approach, due to the contentions provided by cyberwar. Secondly, it is hard to demonstrate a concrete example of two democracies engaging each other in warfare, if the reasons explaining this, as presented by democratic peace theorists, are correct then we could be entering an age of increasing instability as democracies readily engage each other on the cyber battlefield. My articulated question is 'Is Democratic Peace Theory Undermined on the Cyber Battlefield?' Therefore in answer to the initial question, no, in fact it can be more detrimental to security and the problems associated with it.

Democratic peace is a historically proven and appealing solution to the violent and anarchic nature of international relations. However, much of the statistical proof for claims of a democratic peace rest on constrained and narrow definitions of war. Cyberwar introduces a new method of war that negates many of the principles and parameters of democratic peace theory, subsequently putting the validity of a democratic peace in doubt. In order to conclusively assess whether democratic peace is applicable to cyberspace, I shall, firstly, define cyberwar in reference to current debate and the Clausewitzian understanding of war.[1] Secondly I will contrast the characteristics of cyber war to the framework of democratic peace theory. Ultimately democratic peace theory has little applicability to the realm of cyberspace, but, importantly, to date the democratic peace has held, as two democratic states are yet to engage in cyberwar.

"Cyber war will not happen" and "cyber war will happen!" are, two conflicting arguments posed by Thomas Rid and John Stone respectively.[2],[3] Although, as the titles suggest, both are seeking to establish the likelihood of cyber war, the essential disagreement can be seen as does cyberwar constitute war. Thomas Rid claims that, due to the lack violence in a cyber attack it cannot equate to conventional understandings of war, and thus is not.[4] Rid refers to Clausewitz's definition, "war is an act of force to compel an enemy to do our will."[5] The crucial word for Rid is force, which he defines as violence and thus an action of war must pertain an element of lethality.[6] However this seems to be a flawed understanding of war and, as John Stone points out, is historically unfounded.[7] Stone highlights the 1943 bombings of the Bavarian town of Schweinfurt.[8] The

---

[1] Clausewitz, Carl Von, Trans. J. J Graham, *On War*, (New York 2004),p.1
[2] Rid, Thomas, *Cyberwar Will Not Take Place,(*Hurst&Co,2013)pp.xiii-vi
[3] Stone, John, "Cyberwar Will Take Place!" *The Journal of Strategic Studies*, 36:1,(2013),pp.101-108
[4] Rid, Thomas, *Cyberwar Will Not Take Place,(*Hurst&Co,2013)p.2
[5] Clausewitz, Carl Von, Trans. J. J Graham, *On War*, (New York 2004),p.1
[6] Rid, Thomas, *Cyberwar Will Not Take Place,(*Hurst&Co,2013)p.2
[7] Stone, John, "Cyberwar Will Take Place!" *The Journal of Strategic Studies*, 36:1,(2013),p.104
[8] Ibid.

intended aim was to destroy German ball-bearing production capacity.[9] Although over 400 civilians died in these raids, providing Rid's lethality, it was seen as "incidental to the desired goal".[10] The proposition is that, these air raids had no aim of lethality but were clearly acts of war, and thus Rid's requirement of lethal violence is restrictive, even by conventional understandings of war. It is possible to reinforce John Stone's argument with the logic that, if an action of cyberwar results in the "compel(ling)" of an enemy to do the attackers "will" then it arguably constitutes war, at least by a Clausewitzian definition.[11] Essentially, this means that if cyberwar achieves the same result as traditional warfare, it should be considered as war. This is reinforced by the idea that if "breaking and entering" in cyber space, the theft of personal or corporate information, is registered as an equal if not greater crime as physically breaking and entering, then cyberwar that achieves the submission of the opponents will, must equate to a conventional conflict that amounts to the same.[12]

The cyber attacks on Estonia in April 2007 demonstrate this.[13] As the result of the proposed removal of a Soviet war memorial from the centre of Tallinn, Estonia and its online infrastructure came under attack from computers of Russian origin.[14] In context, Estonia was regularly called the "wired state of Europe", with 90% of its domestic financial transactions taking place online.[15] By May 19th Hansabank, Estonia's largest bank, was forced offline.[16] Ultimately to stop these attacks the Estonian government was forced to close down all external Internet traffic, essentially shutting itself off to the rest of the world.[17] Although, clearly, this is not a cyberwar between two democracies, it

---

[9] Stone, John, "Cyberwar Will Take Place!" *The Journal of Strategic Studies*, 36:1,(2013),p.104..
[10] Ibid.
[11] Clausewitz, Carl Von, Trans. J. J Graham*, On War*,(New York 2004),p.1
[12] Chong, Alan, "Information Warfare? The Case for an Asian Perspective on Information operation", *Armed Forces & Society*,40:4,(2014),p.608
[13] Ibid,p.600
[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] Ibid,p.602

demonstrates that a state can force another to act against its own will, by the use of a cyber attack. In this case Estonia closing itself off to the world, causing significant disruption and economic damage. Estonia's cyber space was recognized by Russia as integral to the "wired state", and was targeted for this reason.[18] It is hard to deny, therefore, that cyberwar does not constitute war; if, as this example shows, it has the potential to achieve the same ends desired in a conventional conflict. The retort could be made that the memorial was still removed, demonstrating Estonia did not bow to Russian desires; but this seems naive to the nature of Russian intentions during this period. The attack on Estonia can be seen as a move by Russia to demonstrate its support of ethnic Russian communities in former soviet bloc states, this is highlighted by the 2008 Russo-Georgian war which also involved substantial cyber attacks.[19] However it should be noted that a cyber war such as this would not fall under the traditional definition of war utilized by democratic peace theory, the "correlates of war."[20] Thus the distinction should be established that either the correlates of war are outdated and cannot help in understanding the ever modernizing developments of war, or that cyber war does not constitute as a sufficient example of conflict; it seems on assessment of the above example the later is incorrect.

The logic of democratic peace theory prescribes that democracies do not engage one another in military conflict, due to the nature of democratic systems and the shared cultural norms that reject violence.[21] Cyber warfare introduces several new elements that null these factors, and in so doing raise questions of the validity of democratic peace theory. Democratic peace theory posits that the absence of war between democratic states is a result of "institutional constraints; the restraining effect of public opinion or of the checks and balances embedded

---

[18] Chong, Alan, "Information Warfare? The Case for an Asian Perspective on Infromation operation,"*Armed Forces & Society*,2014,40:4,p.600
[19] Rid, Thomas, *Cyberwar Will Not Take Place,(*Hurst&Co,2013)p.7
[20] Giber, Douglas & Reid, Meredith, "Measuring Alliance: The Correlates of War Formal Interstate Alliance Datatset, 1816-2000"*, Journal of Peace Research*, 41:2(2004)pp.211-222
[21] Layne, Christopher, "Kant or Cant: the Myth of Democratic Peace"*, International Securtity*,19:2,(1992)p.6

in the democratic structures."[22] In cyber warfare, however, the dynamics of conflict have fundamentally changed, negating these explanations. For example the battlefield of cyber war is not inhabited by soldiers but by servers. This subsequently removes the danger to life, and thus it must remove a strong element of public aversion to conflict. Secondly if the conventional elements of war are either removed entirely, or substantially reduced, it will be accompanied by a significant cost reduction.[23] Thus if a nation will not loose "its treasure" (comparatively to conventional war), and there still remains the possibility of gain from a cyber conflict, in the form of prestige or a stronger global position; the assumption that democracies would be unwilling to commit to a conflict, lacks evidence.[24] Ultimately, if "blood and treasure" were not applicable there would be little, if no, restraining effect.[25] This is because these are two, fundamental, war retardants held by democratic peace theorists.

Christopher Layne points out that democratic peace theorist often argue "that the absence of war between democracies is more important than the absence of threats".[26] The validity of this argument, as a result of the weaknesses highlighted above, is now under much greater pressure. Democratic states can now threaten another international actor with cyberwar, without the restraints they were contained by before. The comparatively smaller cost of a cyber attack, in terms of "Blood" and "Treasure", to a conventional one is demonstrated by "struxnet".[27][28] This was a virus, planted by the US, which infected the Iranian nuclear facilities' computer network.[29] This caused an internal explosion by disrupting the separation process of uranium-235.[30] The conventional

---

[22] Ibid.
[23] Farwell, James P.; Rohozinski, Rafal "Stuxnet and the Future of Cyber War Survival" *Global Politics and Strategy*,53:1,(2011)p.27
[24] Layne, Christopher, "Kant or Cant: the Myth of Democratic Peace"*, International Security*,19:2,(1992)p.9
[25] Ibid.
[26] Ibid.p.14
[27] Ibid.p.9
[28] Farwell, James P.; Rohozinski, Rafal "Stuxnet and the Future of Cyber War Survival" *Global Politics and Strategy*,53:1,(2011)p.27
[29] Ibid,p.24
[30] Ibid,p.26

alternative, that could have caused the same level of damage, would have been an airstrike using special munitions, with estimate costs running into millions of dollars.[31] Struxnet was cheap as it "capitalized on code expertise" that already existed.[32] Furthermore no US personnel were put at risk to carry out the operation. Cyberwar thus challenges the assertion that substantial physical and economic loss prevents elected leaders from taking their countries to war with other democratic states. This is because the weight of public antipathy to these loses, is essentially non-applicable in cyberwar; rebuffing the claims that war will not happen between democratic states.

The transparency and legality of democratic states is also claimed by democratic peace theorist to demonstrate why democratic states are less likely to engage in conflict.[33] As a result of this transparency and conformity to international legal norms it is argued that, democratic states have an innate level of trust amongst each other.[34] However, in the cyber world such faith in another states intentions, especially those towards you, is challenged. This is due to the element of deniability that is possible with cyber attacks, that is not possible via conventional methods.[35] For example, operation "Titan Rain", as dubbed by the US, was a wide spread cyber attack on multiple US and UK government departments from 2003-07, that came from Chinese origin.[36] The blame was put solely on PLA by British and American government officials; yet the Chinese government was able to plainly deny these claims due to the attacks untraceable nature.[37] Although again this example is not a conflict between two democracies, it clearly shows that transparency and legality do not apply in cyber space. This

---

[31] Farwell, James P., Rohozinski, Rafal "Stuxnet and the Future of Cyber War Survival" *Global Politics and Strategy*, 53:1,(2011)p.28
[32] Ibid,p.27
[33] Doyle, Michael, "Kant Liberal Legacies, and Foreign Affairs," *Philosophy & public Affairs*,12:3,(1983)p.230
[34] Ibid.
[35] Farwell, James P.; Rohozinski, Rafal "Stuxnet and the Future of Cyber War Survival" *Global Politics and Strategy*,53:1,(2011)p.26
[36] Carr, Jeffery, *Inside Cyber Warfare Mapping the Cyber World* (Sebastopol 2011)pp.4-5
[37] Ibid.

is because a state could perpetrate an attack to disable a government's infrastructure, an act that fulfils the parameters of war, but then deny any involvement. As Chinese government did by arguing they had no part in the attack.[38] Crucially America and the UK were restricted in their response on these grounds, and could not pursue a legal course.[39] Therefore, because the burden of proof in the cyber world is so much greater it could fog up the transparency of democratic states and thus trust in one another would dissipate. Cyberspace is therefore a domain in which, a state could attack another and not be held accountable to international legal norms.[40] The situation has arisen where transparency and conformity to legal norms are no longer relevant, because states can act essentially anonymously. Ultimately, this will challenge democracies' commitment to international law.

Maoz and Russet in "A Statistical Artifact?" state that democratic spirit of "peaceful competition, persuasion and compromise" explains why democracies behave in a "qualatively" different manner towards each other than they do towards non-democracies.[41][42] As the cyber world continues to develop this idea of peaceful competition, on which democratic peace's foundations lie, is increasingly challenged. As a result it is possible to conclude that the apparent stability of democratic peace is not foreseeable. This can be demonstrated by the comparison of the 1923 Ruhr crisis with the 2013 United States National Security Agency's espionage on the state owned Brazilian oil giant Petrobras.

---

[38] Carr, Jeffery, *Inside Cyber Warfare Mapping the Cyber World,*(Sebastopol-2011)pp.4-5.
[39] Arthur, Charles, "US accusations of Chinese hacking Point to eight year spying campaign," *The Guardian*, 19/05/2014,Accessed:17/02/2015
[40] Farwell, James P.; Rohozinski, Rafal, "Stuxnet and the Future of Cyber War Survival" *Global Politics and Strategy*,53:1(2011),p.26
[41] Maoz, Zeev; Russet, Bruce, "Alliance, contiguity, wealth, and political stability: Is the lack of conflict among democracies a statistical artifact?" *International Interactions*, 17:3,(1992)p.246
[42] Layne, Christopher, "Kant or Cant: the Myth of Democratic Peace"*, International Securtity*, 19:2,(1992)p.10

Historically the idea that democracies behave towards one another with a mutual respect has been regularly challenged. Christopher Layne in "Kant or Can't: The Myth of the Democratic Peace" challenged such arguments with the example of the 1923 Franco-German Ruhr Crisis.[43] Essentially Layne claims that, the occupation of the Ruhr valley by France is an example where the inherent respect that democracies have for one another, was not present.[44] The occupation of the Ruhr showed that France's war objective of crippling Wilhelm Germany remained the same, despite the fact that Germany was now a democratic republic. Up to 1923 France had rejected the idea of a new democratic Germany, as they did not believe their security situation had fundamentally changed.[45] "What mattered to France was Germany's latent power", France's attitude toward Germany "displayed none of the mutual respect based on democratic norms and culture" on which democratic peace theory rests.[46] As a consequence the French PM Poincare had no option, if he was to maintain his prime ministerial position, but to occupy the Ruhr as anti-German sentiment was so high in France.[47] The Ruhr crisis provides two problematic situations for democratic peace theorists. Firstly it demonstrates that, should it be politically expedient for one democracy to force itself upon another, as it was for Poincare, it will.[48] Secondly, and more importantly for cyber war, when the situation arises that one democracy is inherently weaker than another (Germany 1923) then it becomes a viable target for other democracies. This is arguably the current situation in cyber space and consequently the cyber battlefield.

In September 2013 it emerged that the U.S had been spying on the Brazilian oil company Petrobras.[49] This provides many parallels to 1923 and is essentially an

---

[43] Layne, Christopher, "Kant or Cant: the Myth of Democratic Peace", *International Securtity*,19:2,(1992)p.30
[44] Ibid.
[45] Ibid,p.31
[46] Ibid,p.32
[47] Ibid,p.30
[48] Ibid.
[49] Antunes, Anderson, "What Are The Chances Of Brazil's State-Owned Oil Giant Going Bankrupt?" *Forbes*,Accessed:5/02/2015

act of corporate cyber espionage by the U.S, against a state owned oil producer.[50] From this it is possible to conclude that the United States, in a similar fashion to France in 1923, does not conform to ideas of mutual respect; instead they sought to understand the "Latent" economic power of Petrobras, and thus the Brazilian government's oil wealth.[51] At this point it is important to acknowledge Moaz and Russet's claim that democratic peace is generated by "peaceful competition, persuasion and compromise", thus the stability of the so called democratic peace, if Moaz and Russet are correct, is on unstable ground, as a result of an increasing turn to the realm of cyber space.[52] The Petrobras incident demonstrates that in cyber space two essential pillars of democratic peace have been removed. This is because the United States has shown that democratic states do not have the inherent respect required of democratic peace theory, when they are operating in the cyber world. Furthermore on the evidence presented it is possible to conclude, if not predict, that democracies such as the U.S would be willing to perform a cyber attack if it enabled some kind of economic benefit. Therefore the growth of the cyber world has simultaneously eliminated the idea of trust between democracies. As a result the likelihood of (cyber)war is much greater.

The counter argument could be made here that Petrobras, despite its majority state ownership, does not amount to a democratic state, hence this example does not undermine democratic peace theory's requisite that democracies hold mutual respect and compete peacefully. However this is one example of many. If, for example, you examine 2013-14 revelations that the CIA and NSA were exercising a "Special Collections Service"(SCS) unit in Berlin monitoring not only Angela Merkel's phone conversations, but also the committee rooms of the Reichstag, the future for democratic peace in the cyber realm is bleak.[53] This

---

[50] Ibid.
[51] Layne, Christopher, "Kant or Cant: the Myth of Democratic Peace", *International Securtity*, 19:2,(1992)p.32
[52] Maoz, Zeev; Russet, Bruce, "Alliance, contiguity, wealth, and political stability: Is the lack of conflict among democracies a statistical artifact?" *International Interactions*, 17:3,(1992)p.246
[53] Smale, Alison; Mazetti, Mark; Sanger David, 'Germany to Oust Top CIA Officer as a Rift Deepens,' *The New York Times,*11/07/2014-Accessed:03/02/2015

example demonstrates that not only do democracies not inherently trust democratically elected leaders, but also the legislative bodies within democratic states. Moreover the SCS program has been in operation across Europe operating in other capitals such as Madrid.[54] What this demonstrates, is that if a democratic state has the ability to do something, as the U.S cyber dominance has allowed in this case, it will do it. Furthermore it demonstrates that it will not be restrained by the articulated parameters of democratic peace theory.

Cyberwar presents a decisive challenge to democratic peace theory. The developing nature of warfare allows the logic of the democratic peace to be disputed. This is because cyberwar is not restricted by the confinements of public opinion, this in turn defeats ideas of transparency and trust between democracies. However, as stated, an example of cyberwar, that in itself, disproves the democratic peace cannot be provided; only examples that indicate the likelihood of future cyberwars between democracies. When two democratic states come into collision on an issue divisive enough for them to question the trust on which democratic peace is orientated, the inherent harmony of democracies will collapse. This is beginning to emerge as the U.S utilizes its cyber hegemony to infiltrate other democratic states, in order to understand their intentions, and true capabilities. What cyberwar reinforces, therefore, is that democracy is still in its founding moments and to conclude that it will create a perpetual peace, is to ignore the possibility of development in what we define as peace and war.

[54] Spiegel Staff, "Embassy Espionage,"*Spiegel Online,*27/10/1013 Accessed:03/02/2015

Bibliography

- Antunes, Anderson, "What Are The Chances Of Brazil's State-Owned Oil Giant Going Bankrupt?" *Forbes*,Accessed:5/02/2015

- Arthur, Charles, "US accusations of Chinese hacking Point to eight year spying campaign," *The Guardian*, 19/05/2014,Accessed:17/02/2015

- Carr, Jeffery, *Inside Cyber Warfare Mapping the Cyber World* (Sebastopol 2011)pp.4-5

- Chong, Alan, Information Warfare? The Case for an Asian Perspective on Information operation, Armed Forces & Society,40:4,(2014),p.600, p.602 p.608

- Clausewitz, Carl Von, Trans. J. J Graham, On War, (New York 2004),p.1

- Doyle, Michael, 'Kant Liberal Legacies, and Foreign Affairs," *Philosophy & public Affairs*,12:3,(1983)p.230

- Farwell, James P.; Rohozinski, Rafal "Stuxnet and the Future of Cyber War Survival" *Global Politics and Strategy*,53:1,(2011)p.24, p.26, p.27, p.28

- Giber, Douglas & Reid, Meredith, 'Measuring Alliance: The Correlates of War Formal Interstate Alliance Datatset, 1816-2000'*, Journal of Peace Research*, 41:2(2004)pp.211-222

- Layne, Christopher, "Kant or Cant: the Myth of Democratic Peace"*, International Securtity*,19:2,(1992)p.6, p.9, p.10, p.14

- Maoz, Zeev; Russet, Bruce, "Alliance, contiguity, wealth, and political stability: Is the lack of conflict among democracies a statistical artifact?" *International Interactions*, 17:3,(1992)p.246

- Rid, Thomas, *Cyberwar Will Not Take Place, (*Hurst&Co,2013) pp.xiii-vi, p.2, p.7

- Smale, Alison; Mazetti, Mark; Sanger David, 'Germany to Oust Top CIA Officer as a Rift Deepens,' *The New York Times,*11/07/2014-Accessed:03/02/2015

- Spiegel Staff, 'Embassy Espionage,' *Spiegel Online,*27/10/1013 Accessed:03/02/2015

- Stone, John, "Cyberwar Will Take Place!" *The Journal of Strategic Studies*, 36:1,(2013),pp.101-108, p.104