Global Policy, August 2017

Cyberwarfare and the Russian Weaponisation of Information in the 2016 US Elections

Er-Win Tan
University of Malaya

Abstract

Whilst much has been written about the use of internet-based viruses as a cyberwarfare weapon to inflict damage on the infrastructure of other countries, one area that has not been examined concerns the manipulation of information to ferment disunity in other countries as an act of political subversion. Such a form of cyberwarfare poses particular challenges due to the difficulty of attributing such weaponisation of information. Furthermore, given that the weaponisation of information does not involve the use of military force, the target of such an action is faced with the difficulty of formulating an appropriate response. Russia's use of its intelligence apparatus to hack the Democratic campaign in the US 2016 Presidential Elections reflected the weaponisation of information itself. Seeking to tilt the election in favour of Donald Trump, Russian weaponisation of information against the US took the form of a three-pronged strategy that had the effect of, firstly, sowing division within the Democratic Party; secondly, damaging the credibility of Hillary Clinton's candidacy for President; and thirdly, arousing far-right sentiments to convince conservative voters in swing-states to support Trump's Republican candidacy. This paper will conclude by examining how democracies may strengthen their political institutions against the application of cyberspace to undertake the weaponisation of information as an act of political subversion.

Policy recommendations

- Russia's use of cyberspace to weaponize information marked an act of political subversion against the democratic institutions of the United States.
- Both the transatlantic alliance, as well as other democracies, must strengthen their defenses against externally-directed weaponisation of information on cyberspace.
- Strengthening cyber-security and firewalls offer only the first line of defence against externally-directed weaponization of information via cyberspace by a skilled cyberwarfare adversary.

- Democratic political institutions must be empowered to maintain constitutional oversight to follow electronic trails that indicate evidence of externally-directed cyber-political subversion.
- Political parties and other democratic institutions must demonstrate transparency and accountability to their constituents to prevent foreign entities from manipulating internal political documents in a bid to skew election results.
- Mainstream media voices must maintain an active and socially responsible role in providing a fair and objective newsfeed that challenges fringe political perspectives and conspiracy theories.

Introduction

The Information Revolution has underscored the centrality of internet-based information as the social currency of the 21st century. This has granted states with an increased array of cyber-based instruments with which strategic coercion can be exercised against their rivals in international politics. This is part of the trend known as cyberwarfare: the utilization of the internet to achieve a state's security objectives. Whilst it is beyond this paper's scope to offer a comprehensive overview of all the various forms of cyberwarfare, of particular interest is the Russian hacking of the US 2016 Presidential Election, which marked the weaponisation of information itself to undertake political subversion of a major democracy. Whilst Russian use of subversion to undermine its enemies is not new – it was widely practiced by the KGB during the Cold War – what is notable is the extent to which cyberspace amplified the impact of weaponized information. Furthermore, Russian cyberwarfare activities against the US in 2016, whilst constituting a hostile act against US interests and undermining US democratic political institutions, fell short of any accepted definition of the use of force.

This analysis is developed in the following three sections, beginning with a brief discussion of the conceptual basis upon which information may be turned into a political weapon. The second section empirically analyzes Russian weaponisation of information in attempting to influence the outcome of the 2016 US Elections. The third section of this manuscript will conclude by examining how democracies may respond to the threat posed by the weaponisation of information on cyberspace.

Cyberspace and The Weaponisation of Information

Clausewitz's conceptualization of war as an instrument of policy envisaged the application of military force against a 'Schwerpunkt' or 'Center of Gravity', commonly understood to refer to a particularly critical physical location on the battlefield, in order to achieve a decisive victory. In contrast, the weaponisation of information through cyberspace does not involve kinetic operations, thus granting the perpetrator the cover of plausible deniability. Such a doctrine may take the form of subversion and manipulation of domestic political forces in the target country. Whilst it remains debatable over the extent to which Russian meddling skewed the election result in favour of Trump, the real damage to the US is to be found in the weakened trust that the American public has in its political establishment, as well as to US credibility in the eyes of the international community.

For the purpose of this manuscript, the application of cyberspace for the weaponisation of information against the civilian population of an adversary state is defined as involving the following components:

i) Objective:

the manipulation of the target population's perception of important political issues (domestically and internationally) in order to damage its political institutions and alliance relations.

ii) Instrument:

the use of cyberspace to inject erroneous, exaggerated or inaccurate information to fringe political websites, to promote a media narrative based on falsehoods and conspiracy theories, thereby sowing discord in the target's civilian polity.

iii) Effects:

a. strengthening internal subversive political forces and hence their ability to damage the target country's political institutions;

b. undermining the credibility of mainstream political voices and political institutions in the target, thereby preventing moderate political opinion and expert analysis from challenging the validity of fringe political views.

The application of information as a weapon poses two particular challenges to the target. First, the abstract nature of information means that the attribution of weaponized information is particularly difficult. Unlike the deployment of combat forces, cyberspace facilitates the movement of weaponized information through a realm that transcends recognized political boundaries and delivering its impact within the target nation. Such attacks can be undertaken through the use of botnets and IP spoofing to throw cybersecurity investigators off-track. Yet, having reached its intended target, such a weaponized form of information can achieve its sender's objectives by damaging the credibility and political reputation of its target, even without the use of kinetic action.

Second, even when cybersecurity attribution has identified a state as the projector of weaponized information, the perpetrator can bring to its defence the principles of freedom of speech and information. As these are pillars on which democratic institutions are founded, a democracy's attempt to retaliate against a purveyor of weaponized information would be condemned as hypocritical, not only by the said perpetrator, but also by media watchdogs, civil rights organizations and public opinion.

Set against this backdrop, the Information Revolution has underscored the centrality of information as a critical organizing principle of contemporary human existence. This has created virtually unlimited opportunities for the establishment of ideologically biased websites, such as Breitbart and Info-Wars, which promote extremist political views and conspiracy theories. The proliferation of fake news sites is particularly serious, given that such entities have no obligation or incentive to maintain a credible reputation. Rather, they prioritise the maximization of viewership, even if this involves the deliberate use of attention-seeking headlines as 'clickbait' to attract the unwary internet user. Bereft of any sense of accountability or social responsibility, yet focused on propagating an ideologically-driven agenda, such websites undermine the democratic process by creating opportunities for foreign powers to inject misinformation into the target's civil society.

As increasing numbers of ideologically biased entities have taken to the internet to propagate their worldviews, the average net-user is thus faced with a bewildering array of channels that purport to broadcast news. The average net-user is not a particularly incisive observer of world affairs, as a result of which comparatively few people have the intellectual skills necessary to separate biased opinions from empirically-proven facts and analysis. As a result, increasing numbers of people on either side of the political spectrum find themselves in an 'echo chamber' in which contrary information, even when presented by expert analysis and reinforced by empirical evidence, is rejected in favour of unquestioning adherence to existing, ideological-based worldviews.

The ignorance of the average internet user is not merely a condition of unquestioning assimilation of world news. Rather, ignorance itself is an opportunity for skilled political operators to exploit through introducing confusion to gaslight the media narrative, thereby preventing objective analysis from reaching the masses. As Gordon Corera noted, 'news may be fake or it may just be slanted, but together the effect is to make people unsure what to believe.'

Russian Meddling in the 2016 US Presidential Elections

In Russia, the doctrine of political subversion and disinformation, also referred to as 'Active Measures', supposedly dates back to Czarist times, with the Okhrana's alleged publication of 'The Protocols of the Elders of Zion', a document claiming a Jewish plan for world domination. Now known to be a forgery, the document had been released as a pretext to justify anti-Jewish pogroms. The political transformations experienced by Russia / the Soviet Union during the 20th century saw further refinement of the weaponisation of information. Foretelling Moscow's long-held willingness to support US Presidential candidates pliable to Soviet interests, a former Under-Secretary of Defense Jan Lodal, has revealed that during the Conference on Security and Cooperation in Europe in Helsinki in 1975, Soviet General Secretary Leonid Brezhnev voiced to US President Gerald Ford that 'that we in the Soviet leadership are supporters of your election as president … And we for our part will do everything we can to make that happen.'

Active measures have continued to remain a core component of Russian covert espionage activities after the collapse of the Soviet Union. The beginning of the 21st century has been characterized by a series of developments that have provided Russia with an opportunity to destabilize the transatlantic alliance and recast itself as a great power. Elected President of Russia in 2000, Vladimir Putin's nationalist agenda was helped by the Bush Administration's preoccupation with the War on Terror, which strained US intelligence resources even whilst Putin invested in the cyberwarfare capabilities of Russia's intelligence agencies, the Federal Security Bureau (FSB) and the Main Intelligence Directorate (GRU). Some flavor of Russian planning for covert intelligence operations was reflected in Aleksander Dugin's 1997 publication of *The Foundations of Geopolitics: The Geopolitical Future of Russia*. Dugin envisaged a strategy of inserting intelligence operatives into the US to exploit longstanding political sentiments in the US, in particular, conservative dislike of the centralization of power in the Federal Governmnt. In a similar vein, Putin's appointment of General Valery Gerasimov as Chief of General Staff of the Russian Armed Forces in November 2012 was followed by the conceptualisation of hybrid warfare that blurs the distinction between peace and war, with particular emphasis on the use of cyberspace as an asymmetric means of influencing events in other countries whilst maintaining a level of plausible deniability.

Russian utilization of the internet as a means for undertaking information warfare was evident during earlier crises with its neighbours. In 2007, pro-Russian websites spread conspiracy theories that the Estonian Government had dismantled a memorial to the Soviet Red Army, in order to incite anger amongst ethnic Russians in Estonia. Following the Euromaidan protests in Ukraine that toppled the pro-Moscow government of Viktor Yanukovych in February 2014, Russian-backed hacker groups such as CyberBerkut and CyberRiot Novorossiya flooded the computer networks of key EU governments to delay a coherent transatlantic response.

Russia's hacking of the 2016 US Presidential Election, however, goes much further than its earlier cyberattacks against its small neighbours. The audacity of Russian interference in the US elections reveals two geostrategic trends of note for policymakers concerned with the implications of cyberwarfare: first, even the most militarily powerful and technologically advanced democracy in the world is not immune to the externally-motivated weaponisation of information; and second, by undermining the credibility of American democracy, the successful weaponisation of information is capable of achieving far-reaching effects on international relations.

Herein, four trends in American society are particularly noteworthy in granting Russia a window of opportunity to undermine the credibility of US democracy during the 2016 elections. First, the election of Barack Obama in 2008 aroused anger amongst ultraconservative Americans, for whom the notion of racial equality remains taboo. Second, this same period was marked by growing disenchantment of large sections of American society due to the increasing rich-poor divide. Alienated by a Wall Street establishment perceived as being out of touch with their economic woes, large numbers of working-class Americans pinned their hopes for an anti-establishment candidate as their champion. A third trend was reflected in the growing Islamophobia and xenophobia in the United States due to media coverage of the brutality of the Islamic State in Iraq and Syria (ISIS) and the exaggerated criminal threat posed by illegal immigrants from Mexico.

The impact of these trends was further amplified by a fourth trend that has been underway in the US for some decades, namely, the increasingly insular outlook of many American adults. This is reflected by an inability of many Americans to understand basic principles about how the US Government works. Emory Professor Mark Bauerlein noted that 'no generation in American history has enjoyed so much access to knowledge … [but] when they give the National Assessment of Educational Progress tests, more than half the 12th graders score 'below basic,' which is roughly a D and an F.' Such a trend is particularly alarming, given that a population that fails to understand basic civics can be easily manipulated through the deliberate distribution of information. If anything, the lack of intellectual curiosity amongst many Americans can lead to distrust of expert analysis. As Tom Nichols noted, 'I think all of these things combined together have created this kind of unfounded and fragile arrogance in people where they claim to know as much as experts.'

Set against this, the backgrounds and policy platforms of three of the contenders for the 2016 Presidential race need to be emphasized, these being Hillary Clinton, Bernie Sanders, and Donald Trump. Clinton, as a former First Lady, Senator and Secretary of State, was seen by many working class Americans as the archetype establishment candidate who would oversee a continuation of existing socio-economic policies. In contrast, Sanders and Trump entered the race as outsiders who pledged to change to the 'business-as-usual' patterns of American politics. Sanders' socialist leanings held significant appeal for working-class Americans who feared that a Clinton Presidential victory would result in a continuation of the rich-poor divide. Amidst these developments, Trump's decision to seek the Republican nomination upended the political calculations of both major parties. Trump's colloquial, demagogical rhetoric enabled him to present himself as being representative of the economically downtrodden. As an outsider to politics, his pledge to 'drain the swamp' of excessive Federal Government spending and Wall Street business interests was taken as a godsend by disillusioned working-class Americans in swing-states. Furthermore, by calling for such controversial measures as banning Muslims from entering the country and building a 'border wall' against Mexico, Trump connected with bigoted sections of American society in conservative-leaning swing states. This backdrop of the US election was noted by Russian intelligence, leading to the development of the following three-pronged weaponisation of information that arguably damaged the Clinton campaign and tilted the elections in favour of Trump.

Dividing the Democratic Party

Shortly after Trump announced his candidacy in late 2015, Russian intelligence agents began intensive communications with Trump's campaign team. In the months that followed, the 'Cozy Bear' and 'Fancy Bear' hacking groups, believed to be organized and supported by the FSB and GRU, penetrated the Democratic National Committee (DNC) databases and identified behind-the-scenes maneuvering to undermine the Sanders campaign. 'Fancy Bear' also undertook a 'spear-phishing' attack against Chairman of the Clinton Presidential campaign John Podesta. Claiming an email security alert, the attack redirected Podesta to providing a new password onto a misleading link that granted 'Fancy Bear' access to Podesta's email account and confidential documents relating to Clinton's campaign. On 22 July 2016, a hacker going by the name of 'Guccifer 2.0' – again believed to be an arm of Russian intelligence – released on Wikileaks some 20,000 emails by senior DNC officials that reflected bias against Sanders. Particularly damaging were statements by DNC Chairperson Debbie Schultz that made personal attacks against Sanders. The timing of this leak was no coincidence –Guccifer 2.0 had deliberately withheld this information in early 2016 to allow the Clinton campaign to secure the number of delegates necessary to win the Democratic nomination, then releasing it on the eve of the DNC's nomination convention to anger Sanders supporters and thus sow discord in the Democratic Party. Further contributing to the discord in the Democratic camp was the presence of the independent Presidential campaigns of Gary Johnson and Jill Stein. Although neither independent had any serious prospect for claiming the White House, both adopted various policy positions that appealed to traditional Democratic as well as Republican voters. In the aftermath of the Wikileaks revelations, significant numbers of traditionally Democratic-leaning communities voted for Trump or the two independents as a 'protest vote' to register their displeasure over the internal corruption of the Democratic Party.

Damaging Clinton's Credibility

Second, Russian hackers also fed Wikileaks erroneous information damaging to the Democratic Party, in the full knowledge that right-wing conspiracy theorists would pick up on such 'news' and rebroadcast them without verification for accuracy. Particularly notorious episodes included the claim that Clinton had demonstrated ignorance concerning the proper procedure for handling classified documents through the use of a private email surfer, the 'Pizzagate' accusation that Clinton and Podesta ran a child sex ring out of a Washington DC restaurant, and the claim by Trump surrogate Roger Stone that Clinton Aide Huma Abedin was connected to the HAMAS terrorist group.

Arousing Far-Right Sentiments

The third prong of Russia's attack took the form of setting up fake online personas in order to flood the media newstream with news that played to the advantage of Trump's aggressive, right-wing demagogical rhetoric. This included the use of botnets and malware to infect internet users' accounts – particularly those residing in conservative-leaning communities in swing-states - with fake news stories that portrayed Clinton as a puppet of the Wall Street establishment. Furthermore, the proliferation of fake online accounts to promote an ideological agenda allowed 'Cozy Bear' and 'Fancy Bear' to engage in 'online flame wars' that undermined the credibility of expert analysis, whilst projecting a skewed media narrative that fit into conservative Americans' existing distrust of left-leaning politics and excessive Federal Government spending.

Conclusion: Defending Against the Weaponisation of Information

Set against Russian weaponisation of information to damage democratic institutions, it is necessary for democracies to acknowledge that although such a doctrine does not involve kinetic action, it is definitely a hostile action that goes beyond mere espionage. Given the rapidly deteriorating public image of the US since the outcome of the 2016 Presidential elections, it is clear that externally undertaken weaponisation of information can have a potentially devastating impact on a nation's interests. How might states respond? Military retaliation is not only grossly disproportionate, but also not justifiable under current international law. Rather, given that the weaponisation of information transfers the Clausewitzian *Schwerpunkt* from the battlefield to civilian politics, the primary defense against such attack has to take the form of the hardening of civilian polities against externally-directed subversion. In particular, the outcome of the 2017 French Presidential elections are a notable comparative study. Amidst fears that the recent spate of ISIS-instigated Lone Wolf terrorist actions would generate support for the far-right Marin Le Pen, the election was instead won by the centrist Emmanuel Macron, in spite of Russian attempts to tilt the election in Le Pen's favour. The defence against the online weaponisation of information should ideally take the form of a three-pronged strategy that consists of 1) the technical strengthening of cybersecurity defenses; 2) strengthening the constitutional and judicial functions of government; and 3) the empowerment of the mainstream media, social networking platforms and other stakeholders to upholding centrist politics and values.

i) Cybersecurity

The weaponisation of information via cyberspace requires that the first line of defense take the form of hardening internet-based government portals, as well as increasing the sensitivity and awareness of civil servants to the full array of cyber-based threats. Four components may be identified, these being:

- The hardening of government firewalls against unauthorized breaches by foreign entities.

- The institutionalization of standard operating procedures and, where necessary, the authorization of multiple cyber-security trained persons to review the online handling of sensitive data. Had Clinton been more circumspect in handling sensitive State Department documents and eschewed the use of a personal server, it would have been difficult for right-wing commentators to accuse her of incompetence over national security. The upgrading of cybersecurity to detect external intrusion, as well as honing the ability of cybersecurity investigators to trace and attribute intrusions.

- The deliberate inclusion of false information on sensitive government and political websites that can be fed to foreign cyberhackers. During the 2017 French Presidential Elections, having anticipated Russian cyberattack plans, Macron's team deliberately created false email accounts and fake data as a 'cyber-ambush' to confuse Russian hackers.

At the same time, however, these measures should not be seen as a panacea in preventing future weaponisation of information. The strengthening of cybersecurity and internet firewalls only mitigates the threat posed, as a sufficiently determined group of hackers will find ways to bypass such defenses. As Adrienne LaFrance noted, 'modern cybersecurity is a constant cycle of breaches and patches … eventually hackers find a new way in.' The very nature of the Information Revolution means that any and all computers linked to the internet are potentially vulnerable to sufficiently motivated hackers. Two additional lines of defense against the weaponisation of information are thus necessary.

ii) Political and judicial Oversight and Political Transparency

Strengthening the political and judicial functions of government consists of three components:

- Outlets to register 'protest votes': During the 2016 US elections, the only opportunity for many Democratic and independent voters to register a 'protest vote' against the DNC was during the actual casting of ballots for the Presidency. In contrast, the fact that the French Presidential election comprised of two rounds – one to select the two most preferred candidates, and a second round to select the President – meant that disgruntled voters could use the first round of voting to register a 'protest vote'. Concurrently, with the prospect of the far-right Marin Le Pen emerging triumphant in the second round, French voters acknowledged the centrist Macron as the more responsible choice for their nation.

- Internal transparency: The Macron team was aware that the Russian weaponisation of information in the US elections relied heavily on the smearing of Clinton with made-up scandals. Accordingly, the Macron team was careful in ensuring that internal documents contained no data that could be used to tarnish Macron. Thus, an attempt by 'Fancy Bear' to discredit Macron with a release of documents claiming that Macron had an illicit offshore bank account was acknowledged by French voters as fraudulent.

- Judicial oversight: John Carlin has identified the need for a 'Dead Man's Switch' that will be triggered automatically in the event that irregularities are detected. The actions of Obama between the election result and Trump's inauguration are reflective of such measure, albeit improvised. In the aftermath of Trump's win, Obama instructed FBI Director James Comey to investigate Russian hacking of the DNC, as well as leaving electronic paper trails that pointed to unusually high levels of suspicious email correspondence between the Trump team and various Russian business interests (many believed to be linked to Russian intelligence). In authorizing FBI scrutiny of the circumstances of Trump's win, Obama's actions made it difficult for the new

White House to credibly dismiss allegations of Russian interference. In attempting to block the FBI investigations by firing Comey, Trump only intensified media and public scrutiny of his ties to Russia.

iii) Other stakeholders

- Looking further afield, the third line of cyberdefense is to be found in strengthening and hardening civilian polities. The following three components to this can be identified:

- Social networking sites: the growing number of social networking sites creates increased forums for the dissemination of information. Such a development creates opportunities for irresponsible demagogues and fringe political perspectives to sow discord in society, thereby underscoring the importance of cracking down on social networking sites that absolve themselves of the responsibility to present accurate news to their followers.

- Mainstream media: it is necessary for mainstream media to uphold their responsibilities and obligations to the public. The mainstream media in France observed a news blackout on the eve of polling during the second round of voting, thereby ensuring that voters could make a ballot choice after due reflection on the candidates' policy positions, without being swayed by inaccurate news.

- Civil society: it is vital that democratic polities are underpinned by an actively engaged citizenry that is willing to challenge and dismiss fringe political views and demagogues. During the 2016 US elections, large sections of American society failed to hold Trump accountable for his divisive, inflammatory rhetoric as well as his inability to articulate a coherent policy agenda, choosing instead to be drawn into his eccentric personal life.

Whilst such measures are anathema to purist advocates of freedom of speech, it should be emphasized that the latter is by no means absolute. Issuing death threats or shouting 'fire' in a crowded cinema are in no way defensible as actions of free speech, and are legally punishable. If anything, it should be noted that even a liberal democracy like Germany has restrictions on the freedom of speech, as reflected in legislation that outlaws symbols of the Nazi regime. More recently, the German Governmen has introduced legislation that requires social networking sites to remove material that incites racism and xenophobia. Set against the willingness of foreign governments to utilize the internet for the weaponisation of information to achieve political subversion of the democratic process, the tension between freedom of speech and safeguarding society from external subversion will require continued debate for the foreseeable future.

Er-Win Tan holds a PhD in International Politics from Aberystwyth University. He is currently a Senior Lecturer with the Department of International and Strategic Studies at the University of Malaya.