The Shifting Nature of Cyberwarfare in Middle Eastern States

Emily Fekete

Oklahoma State University

Abstract:

While some theorists make the claim that "kinetic and traditional military power are losing importance to symbolic and media power," in reality the present military situation is complicated by the variety of tactics used by both governments and civilians in multiple and overlapping war zones. The Middle East has recently been the center of enormous military and media attention regarding the use of many forms of "new" media military operations. However, rather than arguing that online warfare has trumped physical encounters, cyber campaigns must be seen as being deployed in conjunction with on-the-ground military maneuvers. The use of online strategies disperses power and allows for an increasing role by non-state actors in both online and offline spaces of conflict. Drawing from the geographic literature on war, especially Derek Gregory's concept of "everywhere war," examples are offered from Syria, Iran, Gaza, and the Islamic State of Iraq and Syria.

Keywords:

terrorism, conflict, Internet studies, cyberactivism, cyber crime, hacking, Middle East

Introduction

Geographers have recognized the impacts that information technology (IT) has had on the dissemination of information about current events beyond the scale of the local (Adams 2009; Fekete and Warf 2013). As individual knowledge about how to use IT continues to grow across the globe, many people are becoming increasingly involved in the production and distribution of news. Social media and other internet-based technologies have allowed individuals to participate in events on a global scale by either increasing awareness or contributing to cyber campaigns, often undermining state control within societies (Slane 2007). While state-sanctioned military

Corresponding author: Emily Fekete, University of Kansas, 1475 Jayhawk Blvd., Lawrence, KS 66044, USA. E-mail: emilyfekete@gmail.com

cyber units are growing in size and number, the increasingly pervasive nature of IT and the Internet has created an environment for non-state actors to participate in warfare traditionally fought by state military forces. The growth of civilian involvement is particularly true for areas located in the Middle East, where a history of state media censorship is gradually losing ground to the growing populations familiar with the Internet and other technologies.

This article focuses on examples of how states and citizens are taking advantage of digital technologies to participate in cyber conflict. Drawing from the geographic literature on warfare, especially Derek Gregory's (2010) concept of the everywhere war, I will argue that current instances of cyberwar contribute to ongoing debates about the shifting nature of the warfare of today. The idea of what constitutes an act of war is changing rapidly with the development of new technologies such as social media, the Internet, and drones. As more civilians have access to these types of technologies, they increase their potential to attack state institutions, broadening the spectrum of what is included in an act of digital war. With civilian groups such as Anonymous committing acts of cyberwar against a state, and private groups, such as the Syrian Electronic Army, commissioned to commit acts of war outside of the state, the definitions of warfare, terrorism, or crime have become murky. At the same time, it is important to see acts of cyberwar or cybercrime in conjunction with the on-the-ground fighting that continues to occur among states. As this article seeks to show, cyber tactics must be seen as another avenue in which wars already being played out in physical space are occurring.

While there has been an increase in the use of cyber tactics in instances of warfare, cyberwarfare does not outweigh or replace traditional military strategies. After a consideration of the literature on cyberwar, the article will turn to examples of the use of cyber campaigns in recent military endeavors in the Middle East from Israel, Palestine, Syria, Iran, and the Islamic State of Iraq and Syria (ISIS). More information about specific cyber attacks has surfaced in the Middle East following the events of the Arab Spring and the greater proliferation of the Internet in Southwest Asian countries. This article takes a critical look at contemporary events using case studies from the region that fall within the growing spectrum of cyberwarfare: the Israeli/Palestinian conflict and cybercitizen participation, the actions of the Syrian Electronic Army, the growth of ISIS and its cybercaliphate, and the actions of online activists against the state. These events were chosen because they constitute examples of the ways in which it is difficult to classify cyberwar. Information about these events has been gathered and synthesized from a variety of journalistic sources. While the Internet allows for war to occur at almost any time, anywhere, it also disperses power among state and non-state actors, confusing warfare, cybercrime, and hacktivism. In looking at contemporary examples of the use of Internet-based maneuvers, this article seeks to demonstrate that while there is an increase in the number of events labeled as cyberwarfare, as well as an increase in participants in acts of war, digital actions must be seen in conjunction with traditional military violence.

War is everywhere

The geography of warfare has been shifting primarily due to the establishment of new technologies that allow for a variety of tactics to be used that could not be utilized as little as fifty years ago. For instance, the use of drone warfare has seen substantial growth by the US military, with both critics and proponents alleging the positives and negatives of the use of drones for military maneuvers (Shaw 2013). The ethical implications of drone warfare aside, what the latest technologies such as these have done is to open up new spaces of war and to change the landscape on which war is conducted. No longer is war regulated to a frontline battlefield, but instead can occur well outside of the traditional warzone and can include actors who are thousands of miles from the site of conflict.

There is a darker side to the growing interconnectedness the world has been undergoing with the advancement of communications and transportation technologies. Globalization is having an effect on the way war is conceived and conducted (Fekete and Warf forthcoming). Agnew (2005) has argued for a need to critically engage with the traditional notion of sovereignty under the umbrella of globalization. Cyberwar not only allows for states to conduct acts of war covertly and over a great distance, but also includes non-state actors and groups, calling into question the power and control of national territories. For Virilio (1986, 1995, 1999), the increased interaction among nationalistic groups is a product of warfare led by the state as a machine to wage war. As Virilio states, "all human geography is ultimately a product of warfare" (Luke and Ó Tuathail 2000:365). Time-space compression occurs because of the drive by states to conduct war. Virilio sees geopolitics (politics influenced by geographical factors) being replaced by chronopolitics (the politics of time) as advances in technology simply speed up the ability of states to wage war on one another as is the case with increases in projectile speeds, transportation of equipment and personnel, and communications technology. With globalization comes the ability for states to act on one another more quickly and with less friction of distance. The use of cyber methods, as it increases the speed in which actions can occur, further enhances the state's ability to commit acts of war.

Following Graham's (2009) notion of "battlespace," where "everything becomes a site of permanent war" in the city, geographer Derek Gregory uses the term "everywhere war" to explain the ongoing changes that warfare often takes today in its spaces of conduct (Gregory 2010a). For Gregory, the warzone has not just been expanded to urban areas, but also to spaces outside of warzones or even, in the case of drone warfare and terrorist organizations, outside of state borders (Gregory 2010a). It is not unheard of in the geography of contemporary war for an attack to occur well beyond the borders of the warring states. What Gregory calls the boundaries of "frictionless war" are further expanded with the use of remote-controlled drone technology manipulated by soldiers in trailers in the Nevada desert (Gregory 2010b). War, he claims, has become more systematic through the use of computer technology that draws literal targets on grids for drone pilots to hit, mirroring in execution the language of warfare and turning the act of war into on committed by an emotionless machine. The geography of war has been expanded everywhere, bolstering Virilio's arguments that the increased pace in contemporary war further changes the political geography of states.

Not only has the site of war shifted, but the actors involved in military operations are changing as well. Gregory (2010b:166) comments on the rise of private military contractors in the everywhere war, saying "thus these wars are fought not by professional armies but by a volatile mix of para-state and non-state actors, including militias and guerrilla forces, whose alliances and allegiances are notoriously unstable." Today's war is marked by the use of new technology and the neoliberalization of the military to include non-state actors either working alone or as hired guns.

This marked change in direction of the conduct of war is especially observed through the use of cyberwar tactics. Typically defined as a disruption of a country's infrastructure and communications systems through the use of malicious code, cyberwarfare is sometimes perceived as state-sponsored cybercriminal activity (Kerr, Rollins, and Theohary 2010). The very definitions of cyberwar, cybercrime, and cyberterrorism are problematic and ill defined, with many government officials using the terms interchangeably (Fekete and Warf forthcoming). Cyberwar can be defined as a potentially lethal act that disrupts a country's infrastructure (including telecommunications and financial systems) by using malicious computer code. The definition of cyberwar used by the Armed Service Committee of the US House of Representatives is a premeditated attack on noncombatants' data, computer systems, or programs resulting in violence. A cyberterrorist attack must also be politically or religiously motivated (Conway 2002). Many US government officials are frustrated with the overuse of the term cyberterrorism, stating that in most cases the word is misused to represent an act of cybercrime. Similarly, the term "hacking" has recently undergone a shift in meaning from a form of technological play in the 1990s to being equated with cybercriminal activity (notably through the actions of the hacker collective Anonymous) (Krapp 2005; Coleman 2014). Therefore, while the terms cybercrime, cyberterrorism, hacking, and cyberwar are often used interchangeably, they instead lay along a spectrum of questionably violent and destructive online activity with hacking on one extreme and cyberwar on the other.

The very nature of cyberattacks to have vague or hidden origins also confuses the terms as it is difficult or impossible to trace whether an event was state-sponsored or not or if it was politically or religiously motivated. Perspective is also important as someone considered to be a “freedom fighter” or “peaceful hacker” from one side may be considered a cybercriminal or cyberterrorist from the other (consider a US citizen working to dismantle the Chinese firewall). The international group Anonymous perhaps best exemplifies the fluidity of online quasi-criminal behavior. Its members engage in “humorous deviance” for a variety of political causes, some taken as lighthearted pranks (such as an attack on the Church of Scientology) while others are seen as national security threats (Coleman 2014). Not only is the nature of warfare shifting in its power structure, but the definition of what constitutes an act of war and who is able to conduct it is also changing as more actions and actors appear to fit the bill.

The confluence of cyberwar and cybercrime led Rid (2012) to argue cyber attacks are the extensions of previously used warfare tactics such as espionage and sabotage, concluding that cyberwar has never occurred and is unlikely to do so in the future. However, there is disagreement among cyberwar experts, as McGraw (2013) asserts that cyberwar is the inevitable next step on the battlefield. Nevertheless, cyber attacks have the capability to inflict real and lasting damage as well as create states of mass confusion among a population.

The boundaries between the real and virtual worlds are growing increasingly blurry, a reality only further illuminated by cyberwarfare. Whether a cyber-threat is posed by a state or non-state actor, cyber-attacks constitute a challenge to state security. Masked by a labyrinth of servers often located in multiple locations across the globe, it is in the very nature of cyber-attacks for the perpetrators to often remain hidden. The indistinct paths that attacks often take make it challenging for states to retaliate against their assailants, especially given that often cyber attacks are not sanctioned by a particular governmental entity, but rather are the brainchild of an independent hacker collective. As Deputy Defense Secretary William J. Lynn III noted, “Once the province of nations, the ability to destroy via cyber means now also rests in the hands of small groups and individuals: from terrorist groups to organized crime, hackers to industrial spies to foreign intelligence services” (quoted in Kerr, Rollins, and Theohary 2010:3).The global nature of cyber campaigns emanating from individuals and groups poses a challenge to the Westphalian state ideal by cultivating a series of "enemies" that reside outside of the state system. The increase in capabilities for citizen cyber-soldiers opens the door for new ways of governing and policing national territories and also creates new theaters of war. Cyberwarfare shifts the frontline of the battlefield to be located not only on physical battlefronts between states, but also on servers that could be in the Department of Defense or on the computers of hacktivist groups.

The development of military technology, the growing reliance on non-state actors for war aid, and the increased use of cyber operations backs Gregory's (2010a:245) claims of "an emerging model of cyberwarfare that involves both the outsourcing of cyber attacks and the militarization of cybercrime." While some states have their own cyber armies such as China's Unit 61398, Israel's Unit 8200, and the United States' CYBERCOM, other governments are more inclined to hire private cyber groups, sometimes even denying their affiliation, as in the case with the Syrian Electronic Army in Syria or Cybercaliphate, which is associated with the Islamic State of Iraq and Syria (ISIS). There has also been an increase in participation of "citizen soldiers" unassociated with a state, who contribute to warfare by voicing their opinions over the Internet and social media or by committing actual cyber attacks in the name of a targeted group. If war was brought into the home with television in the 1960s, the Internet has in many ways allowed for citizens to actively participate in battle as opposed to passively watch events as they unfold. This article now turns to several recent case studies from the Middle East to illustrate how cyberwar further reveals new directions of warfare and the everywhere war. These case studies were chosen to provide a variety of instances along the blurry spectrum of cyberwar with examples from state and non-state actors.

Recent uses of cyber tactics

The ongoing conflict between Israel and the Palestinians is being waged in both online and offline spaces. Israel has a long history of technology development and the use of electronic means of defense. Israel is unique among

Middle Eastern countries not only as a democratic state, but also in terms of its high technology capabilities. Home to some of the most influential high tech cities in the world, such as Tel Aviv, Israel is a global top spender on research and development as a proportion of GDP. Compared to its Middle Eastern enemies, Israel's internet penetration rate sits at 70.8 percent compared to Iran (55.7 percent), Syria (26.2 percent), and the West Bank (55.4 percent) (Table 1). The statistics in Table 1 point to the fact that many of the states in the Middle East have fairly low Internet penetration rates. The average citizen is unlikely to have access to the Internet on a regular basis in which to develop technological skills. Internet connections and knowledge are likely to lie with those who have the most power, either politically or financially. As a country historically heavily backed by the U.S., Israel has both the political and financial means for a highly developed technological sector.

Country	Internet Users (Dec. 2000)	Penetration Rate (Dec. 2013)
Bahrain	40,000	90.0 %
Iran	250,000	55.7 %
Iraq	12,500	9.2 %
Israel	1,270,000	70.8 %
Jordan	127,300	44.2 %
Kuwait	150,000	75.5 %
Lebanon	300,000	70.5 %
Oman	90,000	66.4 %
Palestine (West Bank)	35,000	55.4 %
Qatar	30,000	85.3 %
Saudi Arabia	200,000	60.5 %
Syria	30,000	26.2 %
United Arab Emirates	735,000	88.0 %
Yemen	15,000	20.0 %
Gaza Strip	n/a	n/a

Table 1: Internet Users and Penetration Rates for Middle Eastern Countries. Source: internetworldstats.com.

As early as 2000, there were reports of Israeli government attempts to overload Hezbollah websites. These early cyber campaigns were met with retaliation by hackers who shut down the Israeli Foreign Ministry's website. During the eight-day conflict in 2012, Hamas was also noted to have utilized cyber tactics by making over 44 million attacks on Israeli government websites. Assaults from Hamas cannot simply be stopped by Israel shutting down its Internet because the Palestinian territories use a different Internet service than does Israel (Ackerman and Alexander 2014).

The Israeli government claims that Hamas does not have sufficiently sophisticated technology to be able to damage its online infrastructure or penetrate Israel's advanced Iron Dome Missile Defense system (Kaplan 2014). However, the continuing conflict has sparked activity from many Palestinian sympathizers, both state actors and those unaffiliated with any specific government. For example, in the days leading up to Operation Protective Edge (the name given by Israel to the 2014 Israel-Gaza conflict), the Syrian Electronic Army (SEA) successfully hacked into the Twitter account of the Israeli Defense Force, posting a message saying two rockets had hit the Dimona nuclear facility and warned of a leak (Halleck 2014; Wofford 2014; Kaplan 2014). The Israeli government was able to regain control of the account within a few minutes and assure followers that the previous tweet was false (Halleck 2014). Another public instance of hacking took place on July 13 when the Israeli Domino's Pizza Facebook page was taken over by anti-Israeli groups. The sympathizers used the website to post pro-Palestinian statements as well as photos of Israelis in hiding, claiming that they would be hitting them with rockets (Blau 2014; Ackerman and Alexander 2014). While these examples do not themselves constitute violence, they effectively spread confusion and fear among the Israeli general public.

Members of the Israeli hacker collective Israeli Elite Force also took to Facebook urging the company to take down the pages of Hamas and Islamic Jihad because they were an "incitement to violence." Facebook complied and removed the pages, though as of this writing the groups Hamas is Terrorism and I Hate Hamas are still active, bringing attention to the fact that owners of online private corporations often inadvertently situate themselves on one side of a conflict through their actions (Blau 2014).

Cyber-attacks on Israeli websites and infrastructure have increased by 500 percent since the escalation of on-the-ground conflict in July 2014 (Gilbert 2014b; Wofford 2014). Cyber offensives against Israel, typically in the form of denial-of-service attacks, increased in number, size, and duration, mirroring the intensification of Israeli bombing of Gaza. It is not clear where the incidents are necessarily originating. At the end of July the Israeli cybersecurity firm AdoreGroup claimed that they linked close to 70 percent of the assaults to IP addresses from Qatar (Shamah 2014). However, the hacktivist group Anonymous claimed credit for taking down several Israeli government websites, including that for Mossad, the Israeli secret service, and the Prime Minister's office (Gilbert 2014a; Frizell 2014). The Twitter account *@AnonymousGlobo* announced their attacks in advance using the hashtag *#opsaveGaza* and calling on others to help. In addition to positing details on how to join, the group also posted lists of over one hundred Israeli websites that they claimed to have successfully taken offline (Gilbert 2014a).Part of the increase in Palestinian support by Anonymous was due to the killing of Tayeb Abu Shehada in the West Bank by an Israeli soldier on July 25, 2014. Tayeb Abu Shehada was killed while wearing a Guy Fawkes mask, the signature apparel of Anonymous (Gilbert 2014b).

Many of the current online incursions in Israel resemble those used by the Cyber Fighters of Izz ad-din Al Qassam who had been linked to Iran after attacking the websites of banks in the US periodically from September 2012 to May 2013 (Goldman 2012; Menn 2013). The Cyber Fighters of Izz ad-din Al Qassam used a botnet, Brobot, to effectively shut down the websites of financial institutions for periods of a few hours to an entire day. While it is clear that Brobot is being used to attack Israeli civilian government agencies, military agencies, and financial services, it is unclear who controls it (Gilbert 2014b). Despite these assaults, there was a drop in occurrences during the brief ceasefire on July 27, leading some people to believe that the assailants are still "adhering to real world calls for ceasefire" (Wofford 2014; Gilbert 2014b). Though citizen soldiers have taken to using cyber attacks to participate in acts of war, it appears that the “rules of war” are being followed by these civilian groups.

Israel and Iran have a history of sending each other cyber threats. The most well-known instance involves the Stuxnet computer worm, launched in 2009 and widely publicized in 2010. Stuxnet is regarded as the most sophisticated cyberwarfare weapon ever deployed. The virus, probably deployed via flash drive or memory stick, is programmed to virtually hide itself for months, recording normal operational procedures, before identifying the optimal time to initiate its destruction sequences (Broad, Markoff, and Sanger 2011). Stuxnet is widely believed to have been developed jointly by the United States and Israel in order to target the IR-1 gas centrifuges at the Natanz uranium enrichment plant in Iran (Markov 2010; Kerr, Rollins, and Theohary 2010). After the initiation of the Stuxnet virus, operational capacity at Iran’s uranium plants dropped by 30 percent, keeping large parts of the plant idle for months and delaying its expansion. Iranian software engineers eventually identified and deactivated the malware, though it is estimated that the worm set back the nuclear program in Iran anywhere from 18 months to two years.

Iran replied to Stuxnet with cyber assaults on U.S. banks and military computers, and boasted it would improve its own cyberwar capabilities. On August 15, 2012, Iran is believed to have initiated a large scale cyber-assault on the Saudi Arabian oil company, Aramco. Using a virus called Shamoon that was likely planted in the Aramco computer network through a flash drive or memory stick, data from 30 thousand machines, approximately three-quarters of the company’s computers, was erased and replaced with an image of a burning American flag (Perlroth 2012).While the attack failed to disrupt oil production as intended, it is regarded as the most destructive cyber initiative against a single corporation (Reuters 2012). Several days after hitting Aramco, on August 27, a similar computer virus was sent to RasGas, the Qatari natural gas corporation. Due to similarities in coding structure it is assumed Iran was behind the RasGas virus as well (Zetter 2012).Iran has also been previously accused by Israeli Prime Minister Netanyahu for launching cyber-attacks on Israel (Kaplan 2014).

Cyber attacks in Israel from the Syrian Electronic Army (SEA) are also not new. The pro-Assad group made up of members of the Syrian Computer Society, a technical organization previously run by Syrian president Bashar al-Assad, was formed in May 2011 as a counterpoint to information being posted by Syrian rebels (Perlroth 2013). After formation, however, the SEA used basic malware codes and a variety of spearphishing techniques (sending emails asking for personal information from a fraudulent source) to target the opposition, often assuming the identities of activists by using usernames and passwords obtained from rebel hostages (Brumfield 2012; Scott-Railton and Marquis-Boire 2013). The SEA also capitalized on the rebel reliance on YouTube videos for publicizing information about the atrocities in Syria by circulating fake videos embedded with malware or using programs designed to look like updates to Flash player or Facebook security (Arthur 2012). Information collected from rebel computers was sent back to servers with IP addresses connected to Syriatel, the telecommunications corporation managed by Assad's cousin in Dubai, confirming that the SEA is likely working closely with the Syrian government despite the President's denial of the partnership (Hopkins and Harding 2013). The most recent targets in Syria have been foreign aid workers who are likely to be working with rebels (Perlroth 2013).

In addition to targeting forces within Syria as well as aiding Palestine, the SEA has been responsible for a variety of attacks on Western media sources. Claiming to punish news outlets for spreading false information about the Assad regime, the SEA hacked the websites to *The Guardian*, Al-Jazeera, BBC, France 24TV, the *Financial Times*, *The Onion*, and NPR and posted propaganda messages in support of the president (Hopkins and Harding 2013). The SEA has also previously hacked Twitter accounts, such as on April 23, 2013 when it posted through the false account of the Associated Press that a bomb had exploded in the White House that left President Obama with injuries (Perlroth 2013). The immediate effect of the false tweet was a 143 point drop in the Dow Jones index for several minutes (Hopkins and Harding 2013).

The Islamic State in Iraq and Syria (ISIS) is an example of a non-state actor committing acts of violence and warfare throughout the Middle East. The group has continued to gain territory throughout parts of Iraq and Syria, has occupied Mosul for close to a year, has cut off water supplies from the Euphrates, and occupied several dams, notably the Mosul Dam. Though Iraqi forces were able to take back the Mosul Dam, ISIS's control of water supplies is a serious threat in an arid landscape. The on-the-ground presence of ISIS within the Arabian Peninsula is mirrored by its online presence used for recruitment and, possibly, cyber attacks.

The online activities of ISIS provide another example of how non-state actors have been using cyber campaigning to gain military advantages. ISIS infamously posted videos on YouTube of the beheadings of Western journalists James Foley and Steven Sotloff, forcing them to make statements in favor of ISIS before being killed. Though similar stunts have been pulled by terrorist groups in the past, including most significantly Osama bin Laden's grainy cave recordings, ISIS marks a distinct shift in that the group has deeply embedded itself in Internet culture for the purpose of attracting new recruits (Ackerman 2014; Graham-Harrison 2015). Videos posted by the militants are in high definition and are made to look like movie trailers. Their use of social media platforms is also vast, even going so far as to post pictures of cats holding AK-47s on Instagram (Ackerman 2014). Videos and other media are widely publicized and distributed by tapping into popular hashtags and posting from multiple accounts (Malik et al. 2014).

Amidst airstrikes from the US and its allies against ISIS that began in August 2014, the US and UK have also responded to ISIS' online presence by suspending Twitter accounts, removing videos showing scenes of murder, torture, and other types of violence, and actively trolling ISIS accounts (i.e., arguing against the posts and creating opposing content) (Malik et al. 2014; Ackerman 2014). Despite the efforts of the US Center for Strategic Counterterrorism Communications, ISIS continues to have a solid online presence that it uses for attracting potential members. As of mid-2015, ISIS is still believed to have the upper hand in its online presence (Mazzetti and

Gordon 2015). Military recruitment has shifted to an online space where the young, the demographic traditionally most likely to be Internet users and most in demand by radical groups, are easily targeted.

In addition to the existing online presence of ISIS used to recruit new members, the group may also be developing its own cyber-army. Dubbed Cybercaliphate, the group claiming to be ISIS sympathizers committed a series of cyber attacks against Western media outlets as well as the US government at the end of 2014 and beginning of 2015 (Peterson 2015). The first suspected instance of an attack by Cybercaliphate occurred in December 2014 against the videogame servers of Microsoft and Sony (Raghuvanshi et al. 2015). In January 2015, the website for Malaysia Airlines was reportedly hacked, replacing the homepage banner with a message that read "ISIS Will Prevail" and redirecting site users to a webpage reading "404 - Plane Not Found, hacked by Cybercaliphate" (Chan 2015; Raghuvanshi et al. 2015). The group was also responsible for hacking the Twitter and YouTube feeds of US Central Military Command (Centcom) in January 2015 writing "I love you ISIS" on the pages and tweeting images of publicly available US government documents (Graham-Harrison 2015). The following month, Cybercaliphate claimed attacks such as the 14 minute takeover of the *Newsweek* Twitter feed, sending out threatening tweets to the US first family, tweets reading "Je suIS IS," a reference to the "Je suis Charlie Hebdo" hashtag used in support of the French political magazine *Charlie Hebdo*, and a message reading "we are destroying your national cybersecurity system from the inside" (Chiacu 2015). A similar takeover of the French TV network TV5Monde also occurred in April 2015 when the station went off-air for close to 16 hours and was replaced with the words "Je suIS IS" and flashing images of ID cards of the relatives of French soldiers involved in operations against ISIS. Cybercaliphate urged the soldiers to remove themselves from on-the-ground actions, further entwining online attacks with offline action (Chappell 2015).

Although cyber attacks from Cybercaliphate have recently slowed, possibly due to concentration of efforts at holding physical territory as they face on-the-ground counterattacks from Iraqi forces, the efforts of the online group should not be overlooked. ISIS and Cybercaliphate are different from other online violent groups because of their "embrace of modern technology, mastery of the difficult art of online propaganda, and appeal to young, computer-literate foreigners including known [criminal] hackers" (Graham-Harrison 2015). Though much of the activity from Cybercaliphate has been equated to online vandalism rather than acts of cyberterror, it is suspected that the group may be capable of greater damage as many of its members are likely operating from outside Syria and Iraq. Anti-ISIS groups such as Western governments, social media companies, and the hacker collective Anonymous have officially declared war on Cybercaliphate. Indeed, Anonymous claims to have attacked 800 Twitter accounts, 12 Facebook pages, and more than 50 email addresses linked to ISIS (Martinez 2015). The case of the online "war" between Anonymous and Cybercaliphate represents actions of two non-state entities committing acts that have the potential to harm citizens, noncombatants and military personnel alike, further blurring the definitions of cybercrime, cyberterrorism, and cyberwar. The fact that a large scale online war is being waged between non-state groups also supports Agnew's challenge that scholars must critically engage with what constitutes sovereignty under globalization and Virilio's notion of chronopolitics as new spaces of war are being created with advanced telecommunications, the victors being the side capable of rapid manipulation of technology.

The events of the Arab Spring also provide an example of the nebulous nature of what constitutes an online "freedom fighter" versus a type of cybercrime. The growing penetration rates of mobile phones in Arab Spring countries (Egypt, Libya, Tunisia) allowed for a wider participation of citizens in the protests, primarily through the use of video technologies (Fekete and Warf 2013). Though more citizens within these states likely participated because of the spread of information through online sources, many of those who took part were outside of these countries and even the entire geographic region. By using a combination of the Internet, social media sites, and traditional news outlets, the actions of activists were broadcast across the globe and supported by people who were not physically involved in the conflicts. During the unrest following the Iranian elections in 2009, for example, there was so much protest activity on Twitter that the media began to talk of a Twitter revolution, although only 0.9 percent of Iranians had Twitter accounts at the time (Morozov 2009). Most of the tweets of outrage were from people located outside of Iran's borders and uninvolved in the on-the-ground protesting. The We Are All Khaled Said Facebook page was started by a Google executive and many of the tweets circulating out of Syria were from local activists and picked up by traditional media outlets who were not allowed into Syria at the time (Fekete and Warf 2013). Anonymous used the hashtag *#OpSaveGaza* to inform people of how to commit cyberattacks on Israeli government websites (Gilbert 2014a). As of August 14, 2014 the hashtags *#GazaUnderAttack* and *#IsraelUnderFire* were used four million and 200 thousand times each, respectively (Finighan 2014).

While simply tweeting about warfare activities does not directly contribute to war itself, it has the ability to incite political response and create a feeling of involvement and confusion (Fekete and Warf 2013). The actions of the Arab Spring activists should be seen in conjunction with the state brutality brought down on citizens involved in the uprisings. On the one hand, in Syria these rebellions developed into a full-fledged civil war. On the other, in the case of Anonymous' actions, it may lead to citizen participation by clicking on links provided with instructions on how to commit a denial of service (DOS) attack. Online activism by citizen participants has the potential to impact and effect on-the-ground fighting by military and state-sanctioned units. The use of social media by citizen activists further intensifies the notion of the everywhere war. Not only does war occur and can be accessed everywhere, but it can also be committed by everyone. Cyberwar opens up the geography of war to create new spaces of warfare and also to establish new players, spreading the power structure of martial activity beyond the scope of the military and the actions of the state.

The development of cyberwarfare has allowed for military action to move beyond on-the-ground tactics and aerial attacks. War can indeed occur everywhere and cyberspace is not immune to the advances of government and citizen actors. Actions occurring in cyberspace often mirror other traditional military attacks in scope and timing, as is evidenced by the slowdown of online attacks during temporary ceasefires in Israel. Cyberwar frequently has the same motives as physical war: to dismantle government infrastructures or terrorize the public. However, cyberattacks are not necessarily committed by state militaries, establishing new networks of wartime activity that invites participation from highly organized sub political groups such as the Cyber Fighters of Izz ad-din Al Qassam or ISIS to loosely organized hacktivist collectives like Anonymous. Due to cyberattacks' ambiguous starting points, what constitutes cyberwar and cybercrime are often distorted, furthering confusion as to who is involved in the conflicts. In a geopolitical context where the Westphalian state system still largely dominates foreign policy, the use of cyber initiatives creates a challenge for maintaining traditional wartime tactics and alliances, especially with the rise of citizen activism.

Conflict zones, cyberwar, and the everywhere war

Today, war can indeed occur everywhere, cyberspaces included. Summing up Gregory's arguments of the everywhere war, warzones are no longer the only active combat spaces during war time. Fighting can, and does, occur anywhere, aided by new technology such as drones and the Internet. The rise of citizen soldiers and online activists further pushes what constitutes military activity to the realm of cyberspace. Cyber motions also demonstrate the neoliberal shift of military control from the hands of the state to private corporations and hands-for-hire, a phenomenon Gregory astutely observes. The general public is increasingly participating in warfare events, either by working directly for or as a subsidiary of the state, or as citizens taking matters into their own hands through social media activism or hacktivist collectives. The new warfare of online spaces has the potential to do much physical destruction. Denial-of-service attacks committed both by the state and by activist groups are likely to confuse and disrupt state governments, theoretically leading to harm against citizens or damage to physical infrastructure and property.

However, in spite of the potential harm to the economy, infrastructure, and billions of dollars of computer technology, cyberwarfare still largely serves as a supplement to conventional military tactics rather than a replacement for on-the-ground action. The war between Israel and Gaza, which began on July 8, 2014, resulted in 2,100 Palestinian deaths, most of them civilians and many of them children. Israel sustained 67 deaths from its advances on Gaza, including 64 soldiers (al-Mughrabi and Lubell 2014). Despite multiple attempts at ceasefires as well as encouragement from Egypt and the United States to negotiate a peace treaty, the reality of rockets being launched from both sides has generated an estimated $6 billion in damages for Gaza and another $2.9 billion for Israel (Piven 2014). Between 425 and 485 thousand people are believed to have been displaced, with many of them fleeing to an already overloaded Jordan (al-Mughrabi and Lubell 2014).

The impacts of physical warfare are not to be understated in a time when the media is increasingly emphasizing the role of IT in warfare and state unrest in the Middle East. Countless Syrians are leaving their country for Jordan as well to escape the bloody rebellion against the Assad regime. In addition to Jordan, the nine million Syrians who have been displaced have taken refuge in other parts of Syria, Iraq, Turkey, Lebanon, and parts of Europe, putting a strain on these states to maintain refugee camps (Syrianrefugees.com). The Syrian conflict, which began in March 2011, has already claimed at least 230 thousand lives, with no end in sight (CNN 2014). Syria has also become a hotbed of recruiting activity for the Islamic State of Iraq and Syria, which claims to have 50 thousand soldiers within Syria (Al-Jazeera 2014). The militant group also maintains that it has 30 thousand soldiers in the territories it took from Iraq. ISIS has been demanding Western nations to end their aerial attacks on Iraq, threating to continue posting YouTube videos of the beheadings of journalists following the video of James Foley as a warning for what will happen to other captives if the strikes are not called off. As of writing, at least 20 hostages have been taken by ISIS (Chulov 2014). The US has responded to ISIS with a series of airstrikes, close to 1,500, as well as continued deployment of ground troops to Iraq to aid Iraqi training forces. On June 10, 2015, the deployment of 450 American advisors to help train Iraqi forces was authorized. The engagement with ISIS is still in its infancy.

While undeniably a threat, cyberwarfare must be looked at in conjunction with traditional war tactics, the speeding up of state power via war as Virilio argues. Death tolls, injuries, and displacement of citizens are very real outcomes of war. Cyberespionage causes disruption of military communications and creates confusion among civilians with access to social media and the Internet. The Internet has also allowed for non-state actors to play a greater role in traditional warfare by permitting hacktivist groups to take war into their own hands and target those entities they deem to be on the wrong side. The reality of warfare today is that it is changing. As Gregory has expressed at length, war is everywhere and the development of cyber tactics and technology have only further opened up the geography of war. War also has the potential to be committed by everyone. Technology has established new ways for governments to wage war, but also for citizens to be involved, either through attacks of their own or by participating in networks of online support. Traditional military activity does still have its place as evidenced by on-going conflicts in the Middle East. The danger of the war of today may be to overemphasize the activities that occur in cyberspace and overlook the realities of physical violence.

Acknowledgements

The author would like to thank the anonymous reviewers for their helpful comments on the manuscript and their literature suggestions and Barney Warf for editing assistance.

References

Ackerman, G. and C. Alexander 2014. Domino's becomes battleground in Hamas cyber onslaught on Israel. Bloomberg News. http://www.bloomberg.com/news/2014-07-17/domino-s-becomes-battleground-in-hamas-cyber-onslaught-on-israel.html, accessed August 14, 2014.

Ackerman, S. 2014. Isis's online propaganda outpacing US counter-efforts, ex-officials warn. The Guardian. http://www.theguardian.com/world/2014/sep/22/us-battle-counter-isis-propaganda-online-officials-warn, accessed September 25, 2014.

Adams, P. 2009. Geographies of Media and Communication. Oxford: Wiley-Blackwell.

Al-Jazeera 2014. Islamic State has '50,000 fighters in Syria'. Al-Jazeera. http://www.aljazeera.com/news/middleeast/2014/08/islamic-state-50000-fighters-syria-2014819184258421392.html, accessed August 21, 2014.

al-Mughrabi, N. and M. Lubell 2014. Gaza war wages on, Hamas says Israel tried to kill its military chief. Reuters. http://news.yahoo.com/gaza-war-resumes-deadly-strikes-rocket-fire-005426636.html., accessed August 21, 2014.

Agnew, J. 2005. Sovereignty regimes: Territoriality and state authority in contemporary world politics. Annals of the Association of American Geographers 95(2):437-461.

Arthur, C. 2012. Syrian activists targeted by fake YouTube. Guardian Online. March 20, http://www.guardian.co.uk/technology/2012/mar/20/syrian-activists-fake-youtube, acessed July 23, 2013.

Blau, U. 2014. The Israeli hacktivists cyberwar in Gaza. Mashable. http://mashable.com/2014/07/18/israeli-hacktivists-gaza/, accessed August 14, 2014

Brumfield, B. 2012. Computer spyware is newest weapon in Syrian conflict. CNN Online, February 17. http://www.cnn.com/2012/02/17/tech/web/computer-virus-syria, accessed July 23, 2013.

Chan, K. 2015. Malaysia Airlines Website Hacked By Lizard Squad. Huffington Post Online. http://www.huffingtonpost.com/2015/01/26/malaysia-airlines-website-hacked_n_6544412.html, accessed May 27, 2015.

Chappel, B. 2015. French TV Network Hacked By 'Cyber Caliphate' Group. NPR Online. http://www.npr.org/sections/thetwo-way/2015/04/09/398492643/french-network-tv5monde-is-hacked-by-cyber-caliphate-group, accessed May 27, 2015.

Chiacu, D. 2015. #CyberCaliphate hacks into Newsweek's twitter account. CS Monitor Online. http://www.csmonitor.com/World/Latest-News-Wires/2015/0210/CyberCaliphate-hacks-into-Newsweek-s-twitter-account-video, accessed May 27, 2015.

Chulov, M. 2014. Islamic state militants seize four more foreign hostages in Syria. The Guardian. http://www.theguardian.com/world/2014/aug/20/islamic-state-isis-foreign-hostages-syria-aleppo, accessed August 21, 2014.

CNN 2014. Syria civil war fast facts. CNN World. http://www.cnn.com/2013/08/27/world/meast/syria-civil-war-fast-facts/, accessed August 21, 2014.

Coleman, G. 2014. Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous. London: Verso Books.

Conway, M. 2002. Reality bytes: Cyberterrorism and terrorist 'use' of the Internet. First Monday 7(11).

Fekete, E. and B. Warf 2013. Information technology and the "Arab Spring." Arab World Geographer. 16(2):210-227.

Fekete, E. and B. Warf Forthcoming. Emerging geographies of cyberwar and cyberterrorism. Space and Polity.

Finighan, A. 2014. Gaza and Israel: war of the hashtags. Aljazeera. http://www.aljazeera.com/programmes/insidestory/2014/07/who-winning-social-media-war-over-gaza-201472217242566235.html, accessed August 14, 2014.

Frizell, S. 2014. Off the battlefield, hackers are waging war against Israel and Palestine. Time. http://time.com/3089473/israel-gaza-hackers/, accessed August 14, 2014.

Gilbert, D. 2014a. Anonymous continues cyber attacks on Israeli government websites knocking Mossad and IDF offline. International Business Times UK. http://www.ibtimes.co.uk/anonymous-continues-cyber-attacks-israeli-government-websites-knocking-mossad-idf-offline-1459689, accessed August 14, 2014.

Gilbert, D. 2014b. Iran-linked botnet helps drive cyber attacks against Israel up by 500 percent. International Business Times UK. http://www.ibtimes.co.uk/iran-linked-botnet-helps-drive-cyber-attacks-against-israel-by-500-1460178, accessed August 14, 2014.

Goldman, D. 2012. Major banks hit with biggest cyberattacks in history. CNN. September 28. http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html?hpt=hp_t3, accessed August 5, 2013.

Graham, S. 2009. Cities as battlespace: The new military urbanism. City13 (4):383-402.

Graham-Harrison, E. 2015. Could Isis's 'cyber caliphate' unleash a deadly attack on key targets? The Guardian Online. http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race, accessed May 27, 2015.

Gregory, D. 2010a. The everywhere war. Geographical Journal, 177(3):238-250.

Gregory, D. 2010b. War and peace. Transactions of the Institute of British Geographers. 35:154-186.

Halleck, T. 2014. Syrian Electronic Army hacks Israel defense forces twitter, falsely claims nuclear reactor leak. International Business Times. http://www.ibtimes.com/syrian-electronic-army-hacks-israel-defense-forces-twitter-falsely-claims-nuclear-reactor-1619314, accessed August 19, 2014.

Hopkins, N. and L. Harding 2013. Pro-Assad Syrian hackers launching cyber-attacks on western media. The Guardian, April 29. http://www.guardian.co.uk/world/2013/apr/29/assad-syrian-hackers-cyber-attacks, accessed July 23, 2013.

Howard, P., and Hussain, M. 2011. The role of digital media. Journal of Democracy 2(3):35-48.

Kaplan, R. 2014. Cyber warfare: the next front in the Gaza-Israel conflict? CBS News online. http://www.cbsnews.com/news/cyber-warfare-the-next-front-in-the-israel-gaza-conflict/, accessed August 14, 2014.

Kerr, P., J. Rollins, and C. Theohary 2010. The Stuxnet computer worm: Harbinger of an emerging warfare capability. Washington, DC: Congressional Research Service. http://pubs.mantisintel.com/R41524.pdf, accessed August 14, 2014.

Krapp, P. 2005. Terror and play, or what was hacktivism? Grey Room (21):70-93.

Luke, T. and G. Ó Tuathail 2000. Thinking geopolitical space: The spatiality of war, speed and vision in the work of Paul Virilio. In Thinking space. M. Crang and N. Thrift, eds. Pp. 360-379. London: Routledge.

Malik, S., S. Laville, E. Cresci and A. Gani 2014. Isis in duel with Twitter and YouTube to spread extremist propaganda. The Guardian. http://www.theguardian.com/world/2014/sep/24/isis-twitter-youtube-message-social-media-jihadi, accessed September 25, 2014.

Martinez, M. 2015. Cyberwar: CyberCaliphate targets U.S. military spouses; Anonymous hits ISIS. CNN Online. http://www.cnn.com/2015/02/10/us/isis-cybercaliphate-attacks-cyber-battles/, accessed May 27, 2015.

Mazzetti, M. and M. R. Gordon 2015. ISIS is winning the social media war, US concludes. New York Times Online. http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?partner=rss&emc=rss&_r=0, accessed June 15, 2015.

McGraw 2013. Cyber war is inevitable (unless we build security in). Journal of Strategic Studies 36(1):109-119.

Menn, J. 2013. Cyber attacks against banks more severe than most realize. Reuters, May 18. http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518, accessed August 5, 2013.

Morozov, E. 2011. The net delusion: The dark side of Internet freedom. New York: Public affairs.

Perlroth, N. 2013. Hunting for Syrian hackers' chain of command. New York Times. May 17, p. B1.

Perlroth, N. 2012. In cyberattack on Saudi firm, US sees Iran firing back. New York Times. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all, accessed August 20, 2014.

Peterson, A. 2015. Newsweek Twitter account hijacked by pro-Islamic State group. Washington Post Online. http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/10/newsweek-twitter-account-hijacked-by-cyber-caliphate/, accessed May 27, 2015.

Piven, B. 2014. $6B in damage: Gaza economy reels from four weeks of war. Al-Jazeera America. http://america.aljazeera.com/articles/2014/8/5/fixing-gaza-economy.html, accessed August 21, 2014.

Raghuvanshi, G., P. Newley, and J. Ng 2015. Malaysia Airlines Website Hacked by Group Calling Itself 'Cyber Caliphate'. Wall Street Journal Online. http://www.wsj.com/articles/malaysia-airlines-website-hacked-by-group-calling-itself-cyber-caliphate-1422238358, accessed May 27, 2015.

Reuters 2012. Aramco says cyberattack was aimed at production. New York Times. http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0, accessed August 20, 2014.

Rid, T. 2012. Cyber war will not take place. Journal of Strategic Studies 35(1):5-32.

Scott-Railton, J. and M. Marquis-Boire 2013. A call to harm: New malware attacks target the Syrian opposition. The Citizen Lab, June 21. https://citizenlab.org/2013/06/a-call-to-harm/, accessed July 23, 2013.

Shamah, D. 2014. Qatari tech helps Hamas in tunnels, rockets: expert. Times of Israel. http://www.timesofisrael.com/qatari-tech-helps-hamas-in-tunnels-rockets-expert/, accessed August 14, 2014.

Shaw, Ian G. R. 2013. Predator empire: The geopolitics of US drone warfare. Geopolitics. 18 (3):536-559.

Slane, a. 2007. Democracy, social space, and the Internet. University of Toronto Law Journal 57:81-104.

Syrianrefugees.com 2014. Home. http://syrianrefugees.eu/, accessed August 21, 2014.

Virilio, P. 1986. Speed and politics. New York: Semiotext(e).

Virilio, P. 1995. The art of the motor. Minneapolis: University of Minnesota Press.

Virilio, P. 1999. The politics of the very worst. New York: Semiotext(e).

Wofford, T. 2014. Hackers attack Israel as Israel attacks Gaza. Newsweek. http://www.newsweek.com/hackers-attack-israel-israel-attacks-gaza-263256, accessed August 14, 2014.

Zetter, K. 2012. Qatari gas company hit with virus in waves of attacks on energy companies. Wired. http://www.wired.com/2012/08/hack-attack-strikes-rasgas/, accessed August 20, 2014.