Looking for Insurgency in Cyberspace

Jakub Drmola

This study explores the rapidly developing area of conflicts in cyberspace. Its main objective is to outline the concept of cyber-insurgency, which has so far been missing from academic investigations. In addition, this work examines other types of conflicts present in cyberspace, including cyber-warfare, hacktivism and cyber-terrorism. Drawing key distinctions between these conflicts and cyber-insurgency enables us to formulate cyber-insurgency as a stand-alone concept. To this end, I base crucial features of insurgency on the work of David Galula. Applying this standard and traditional approach to the realm of cyberspace raises specific issues about violence and – more importantly – space itself. Finally, this study proposes reasons for the absence of cyber-insurgency from the current political scene and points to conditions for its future emergence.

Keywords: cyberspace, insurgency, hacktivism, cyber-insurgency, cyber-warfare, cyber-terrorism

Introduction

The early decades of the 21st century have seen a remarkable upsurge in the use of cyberspace during conflicts. While fast-spreading malware and financial cybercrime were common even towards the end of the previous century, recent years have witnessed the first coordinated and substantial cyber-attacks during an inter-state war, the first ever use of malware to remotely sabotage mechanical industrial equipment, the sudden rise of hacking by non-state actors for political ends and an equally sudden spate of revelations about the extent of cyber-espionage conducted by national agencies. This would suggest that the era when force is used in cyberspace has finally dawned.

Scan this article onto your mobile device

At the same time, some phenomena such as cyber-terrorism are nowhere to be seen despite having been predicted long ago. Physically

destructive cyber-attacks remain extremely rare, and losses are usually either financial or to the victim's reputation. Although some truly novel forms of cyber-attacks have occurred and new political uses of cyberspace have taken shape, they have often lacked any successors. If this is the dawn, then it seems that only the very first light is visible.

Against the backdrop of cyberspace's growing prominence in matters besides commerce and entertainment, this study attempts to explore one kind of conflict which often evades attention: cyber-insurgency. Insurgencies are a very common type of discord and one prevalent across the Asian and African continents. Their potential transformation through the influence of cyberspace, thus, deserves some thought.

The first section of this work discusses various forms of political conflict and sources of threats that have been enhanced or transformed by cyberspace's emergence. An attempt is then made to place the concept of cyber-insurgency among these concepts by looking for both common and distinctive traits. These reflections are mostly based on Galula's writings on insurgency.[1] After laying out the basic parameters of cyber-insurgency, I seek to explain its absence from the current scene and look at the conditions which would allow it take root. Finally, I add some observations about the form that cyber-insurgency is likely to take.

Conflicts in Cyberspace

It is not yet entirely clear how cyberspace actually affects human activities such as war, politics and crime. And it is even less obvious how they will be transformed in the future. Some phenomena – cybercrime, for instance – seem to involve a simple expansion into this new territory. Their actors, whether individuals or organised criminal groups, have added new tools and new methods to their existing repertoire to accomplish exactly the same goals that they were striving to achieve before. In other words, the crime has been "enhanced" by the addition of cyberspace and not replaced by a new and different phenomenon . This is a change in scope and breadth and not in substance.[2]

So-called hacktivism (included here despite its lack of the popular "cyber" tag) seems to be a similar case of the fairly straightforward expansion of traditional politics into cyberspace - an adaption for the Internet age. Once again, new methods have been adopted and new tools are being used to achieve pretty much the same goals. The already apparent similarities between politically motivated Distributed Denial of Service

attacks (DDoS) and regular street protests are made even starker by their often concurrent execution by disgruntled groups. Defacements of websites and vandalism of physical billboards also bear close resemblance to one another, and both actions aim to show disagreement or promote a different political message. Protests against the Anti-Counterfeiting Trade Agreement (ACTA),[3] against the Church of Scientology,[4] as part of the Occupy Movement[5] or even within the Arab Spring[6] are the most visible examples of this trend of political actors coming together in time but not in space. Old and new protest methods differ simply in that the first occupies physical space (streets, squares, buildings) while the seconds happens in cyberspace (via servers, data links, information systems). But this is only a difference in means and not in purpose.

One of the most discussed forms of human conflict which could potentially be transformed by cyberspace's involvement is, of course, war. Cyberspace is sometimes deemed the "fifth domain," meaning the fifth type of space where military operations could be conducted.[7] Military operations in cyberspace are, thus, called cyber-warfare. Unfortunately for scholars (and fortunately for almost everyone else), there have been very few opportunities to study this kind of warfare. The primary reason is that even before cyberspace had become a potential venue for inter-state warfare, fully modernised states had all but ceased to wage war against each other. Most wars so far have taken place among states for whom cyberspace does not offer many meaningful targets and whose capabilities in this respect are insufficiently developed.[8] The only notable exception is the 2008 war between Russia and Georgia, and it has been thoroughly analysed and invoked as a harbinger of what is to come.[9]

The lesson so far seems to be that in an inter-state war, cyberspace would play more of an ancillary role akin to that of space-based systems.[10] This essentially means that it would support and enable the increased effectiveness of traditional forces by, among other things, disrupting enemy communications (both internal and external).[11] This concurrence of warfare across several domains is both similar to the hacktivism example and a critical part of the whole cyber-warfare concept.

The increasing proliferation of automated industrial systems and networked infrastructures (e.g. power grids, transport systems, financial institutions, etc.) coupled with growing awareness of their vulnerabilities raises the prospect of a cyber-attack that could break through the "kinetic barrier." Such an attack might, in theory at least, cause significant

physical damage and potentially the loss of life. Nevertheless, with the exception of Stuxnet,[12] no truly physically destructive cyber-attack has yet been positively documented.[13] Like the Georgian War of 2008, the Stuxnet attack of 2010 can perhaps, thus, be considered a sign of things to come. At the same time, while it demonstrated the scope for the physical destruction of industrial systems, Stuxnet was in some ways more divorced from the traditional concept of war than the Georgian example. There was no state of war between the countries involved; there were no concurrent physical engagements. This was a covert (i.e. hidden and deniable) effort to sabotage the Iranian nuclear enrichment program, an act perhaps more political in nature than military.

This kind of cyber-sabotage and cyber-espionage is quite possibly even more complicated than cyber-warfare, in part because it is currently happening and constantly evolving to respond to new threats and opportunities. Outside the high-profile Stuxnet case, information security corporations have discovered a whole slew of covert information-collecting malware (individual instances have names like Flame[14], Duqu[15] and Red October[16]). On top of this, long-term efforts to exploit phishing or directly hack into and extract information from the systems of military industrial and technological companies have been observed and documented. They are usually subsumed under Advanced Persistent Threat (APT) phenomena. These covert attacks make good use of cyberspace's natural attributes – in particular, anonymity and global reach. But these same attributes also make any systematic research quite problematic: since these attacks often remain undiscovered for several years, they can hardly be ascribed to any specific actor, and their ultimate goal can be exceedingly difficult to infer from the available evidence.

It is worth noting that though we can observe a definite upswing in these types of operations, they are not an entirely new type of development. Intelligence services all over the world have been engaging in sabotage and espionage since long before the advent of the Internet and cyberspace. In other words, this is a new form of an already existing activity, rather than the manifestation of a new phenomenon.

Last but not least is the case of cyber-terrorism, which is also quite possibly the most controversial type of cyber-conflict. Consensus on what cyber-terrorism actually means is even harder to come by than is the case with any of the previously discussed phenomena. On a very basic level, we can discern two opposing interpretations of cyber-terrorism.

The first might be shorthanded simply as "terrorists using the Internet." This would include activities like using email to communicate, making websites to spread propaganda and share guidance and perhaps using social media to recruit new members and sympathisers.[17] The second view understands cyber-terrorism as acts of political violence that aim to spread fear and are accomplished – and not just facilitated – using cyberspace tools like computer networks and information systems.[18] These acts might, for example, include hacking into a dam's control systems and flooding towns downstream while at the same time demanding territorial independence or other political concessions. Using conventional explosives to destroy the same dam and achieve the same political goal while tweeting about it would, thus, not be cyber-terrorism on this understanding.

The first approach and its variations have the disadvantage that they are extremely inclusive to the point of uselessness. So many activities can be covered by this definition of terrorism that the meaning of the term may be entirely diluted. The disadvantage of the second and narrower approach is that it does not currently capture a single real case of cyber-terrorism. To date, there has been no politically motivated cyber-attack so violent or damaging that it would really bear comparison to an act of physical terrorism – a suicide bombing, for instance – in terms of the fear instilled in its audience. Unlike cyber-warfare and cyber-sabotage, cyber-terrorism has not yet shown signs that it is looming.

The popular line, of course, is that "it is not matter of *if*, but *when* we experience the first true cyber-terrorist attack." And this may very well be the case. After all, most other human activities and forms of conflict seem sooner or later to expand into cyberspace. If terrorism is simply a more violent and asymmetrical form of political conflict, then there is nothing to suggest that it would be fundamentally different to other acts and somehow incapable of taking advantage of this new environment. At the same time, it is important to keep in mind that this expansion has not yet happened, at least if we adhere to the narrower definition of cyber-terrorism.

The Absence of Cyber-insurgency

The incidence of these different types of cyberspace activities varies wildly. Some are exceedingly rare or virtually non-existent and discussed

mainly as possible future scenarios. This is the case for cyber-terrorism, cyber-sabotage and perhaps cyber-warfare. Others like cybercrime or cyber-espionage can be very common. Hacktivism, despite being a relatively recent addition to this "cyber-zoo," has quickly become commonplace. The key difference between these activities lies not in the nature of the entity behind the action, but rather in the tools involved and the effects desired. The need to break through the kinetic barrier seems to be what is holding back the proliferation of some activities.[19] But while achieving physical results remains difficult, both state and non-state actors have become proficient at routinely disrupting communication channels and extracting and disseminating information. The absence of inter-state cyber-warfare also comes down to the lack of conducive wars, with peacetime espionage in cyberspace basically serving as a substitute.

So where does this leave cyber-insurgency? In these conditions, it has a similar profile to cyber-terrorism - particularly in the sense that it is not a phenomenon we now see occurring, but one we might expect to encounter in the future. This is based on the general observation that existing forms of conflict tend to take advantage of the opportunities that cyberspace offers. Insurgency certainly exists as a kind of conflict and so it follows that cyber-insurgency should hover somewhere on the horizon.

But while many pages of journals and other media have been devoted to cyber-warfare, hacktivism, covert actions and even cyber-terrorism, surprisingly little attention is being paid to the issue of insurgency in cyberspace. Even Dorothy Denning seems to skip insurgency in her axis of increasingly destructive political activities, jumping straight from hacktivism to cyber-terrorism.[20]

The little that can be found on this topic often describes how pre-existing insurgents might use and exploit the Internet to advance their goals, deploying websites or social media to communicate and mobilise.[21] This approach to cyber-insurgency basically mirrors the first approach to cyber-terrorism set out above and is probably too broad. Some commentaries are more specific and innovative but lean towards equating cyber-insurgency with another already existing concept such as hacktivism[22] or else analysing cyber-warfare through the prism of insurgency.[23] While such contributions can be very insightful, none of them really delves into cyber-insurgency as a concept or explains its absence from the current scene.

Cyber-insurgency's Distinctive Features

For those trying to deduce what insurgency in cyberspace might look like or why it seems to be absent, exploring related human behaviours which have been transformed or enhanced by the advent of cyberspace is only one part of the task. The second, and no less important, step is to look at insurgency itself and lay bare its core features and principles. This should enable us to infer how – and under what conditions – insurgency might be influenced by cyberspace.

Fortunately, the research on insurgency is well-established and replete with established works. For the purposes of this review, I focus on Galula's *Counterinsurgency Warfare* as the primary source of insights about insurgency. Galula's work deals with the conflict from both sides; it is pertinent and has stood the test of time. Despite being written in 1964 (which some might view as a shortcoming), it is still being referenced today by scholars and practitioners.[24] This also means that it is not overwhelmed by recent and very specific experiences from Afghanistan and Iraq, which tend to dominate current thinking on insurgency. Instead, it draws on a wider set of conflicts in various parts of the world. Naturally we need to allow for several historical shifts and technological advances which have occurred since Galula wrote this work, but its principal points and observations on the nature of insurgency remain valid.

Compared to war, insurgency differs in several key respects. For a start, it refers to an internal and highly asymmetrical conflict that challenges a current authority. And it is not only the asymmetry of the fighting forces which matters. Insurgents usually lack financial and industrial resources, control over media, transport, any executive or legislative power, diplomatic recognition and sometimes even international support. Cyber-insurgents can also be expected to occupy a much weaker economic and political position than their opponents. This difference in valuable assets is, however, perhaps slightly less pronounced in cyberspace due to its open nature and more easily obtainable and affordable tools. Insurgents are far closer to procuring state-of-the-art computer hardware and software than to operating their own aircraft carriers.

But the asymmetry cuts both ways. Insurgents are crucially free of the heavy burden to maintain order and a stable economy across a country. One of the pillars of their overall strategy is to make this burden even

heavier so that ideally the central authority will crumble under its load. Natural laws teach us that general disorder (also called entropy) is an organic state of affairs and tends to increase within a given system over time.[25] It is therefore always more demanding and expensive to counter this natural tendency by promoting order rather than it is to "go with the flow" and promote disorder. Undermining the government's efforts to run the country by promoting chaos is, thus, a prominent feature of insurgency and a very efficient way to erode state power and authority. This feature can easily be translated into cyberspace. Services provided by state institutions and their infrastructure can, in principle, be targeted during a cyber-insurgency to gnaw away at the regime's authority.

Additionally, insurgents may – and should – occupy the ideological high ground, invoking the abstract power of a political cause without being restrained by tangible obligations. They are also the only side which can initiate a conflict since there can be no counter-insurgency without the insurgency it is opposing. In a traditional inter-state war, the sides are more symmetrical – or at least comparable – in capabilities, resources, goals and responsibilities, and each of them can initiate the conflict.

Another key distinction from war is that insurgency is fought over control of the population. The aim of insurgents is to take control of the people and so secure victory in a protracted struggle. For any regime, the population is a source of both power and legitimacy, and its approval or at least passive submission is needed if that regime is to remain in control. Therefore, the goal of the insurgents' cause is to pull the population away from the central authority without needing to directly overpower its entire military force. In contrast, in an inter-state war, the objective is usually to destroy the enemy's military power and seize control of its territory in order to enforce one's will.

This raises the intriguing issue of space itself.[26] Traditional physical wars between states are fought in all accessible domains because that is where their military assets are located and where they project their power. In some wars, national navies or air forces can exert crucial influence over the whole conflict by achieving decisive superiority in "their" domain. Such superiority can then be leveraged to critically disrupt the opponent's operations in other domains (by means of long-range bombardment or direct combat support, for example). But virtually no fighting takes place in the air or at sea during insurgencies. These

domains may be used by counter-insurgent forces for logistical reasons or support, or insurgents may try to attack and disrupt them, but there is no symmetrical and systematic struggle over their control.

There is a key reason why these domains are not central: they are not where the population lies. There is no one living in the air, at sea or out in space over whom insurgents could fight. Insurgency can only exist where the people permanently live. Even if insurgents managed to take control of some section of airspace or sea (which is hardly achievable given the asymmetrical nature of the conflict and their inadequate resources), they would not benefit from this beyond being able to use the space to move troops and supplies. Insurgencies are primarily land-based conflicts because land is where the people are.

So, if it is the lack of a permanent population that currently prevents outbreaks of insurgencies in the air, at sea and in the orbit around the Earth,[27] where does this leave cyberspace? Can insurgencies occur there at least in theory? In other words, do people live in cyberspace such that insurgents might fight over them in the near future?

From a strictly physical point of view, the answer is obviously a resounding "no" – people do not live in cyberspace and so insurgencies cannot take place there. Cyberspace is basically notional and immaterial (despite being enabled by an infrastructure that is absolutely material); it is physically inaccessible to the solid body of a human being. As such, it is impossible to live in cyberspace in the same sense that one lives on land.

But it is an entirely different matter when one considers cyberspace in a more abstract context. People do spend large amounts of time "in" cyberspace. They work there; they seek entertainment there; they communicate; they even engage in politics and – crucially – they form communities across cyberspace which do not respect the physical boundaries or nationalities of their members. Therefore, there are, in some sense, politically active communities "living" in cyberspace that neither overlap nor are mutually exclusive to physical communities. They emerge more out of common interests and beliefs than shared ancestry or neighbourhoods. In some instances, this may even lead to physical relocations when members of communities originating in cyberspace converge in the same place, thus closing the gap between cyberspace and physical space even further.[28]

Under these conditions, cyberspace looks like a domain where it might be possible for insurgents to battle states and governments for

control over the segment of population that resides online. And this is basically what some hacktivists are already doing. Cyberspace has now spawned groups which use "local" tools to undermine existing central authorities and win the support of the people. Anonymous, an entity probably better described as a broad movement than an integrated group, may well be the best example of this development, but it is far from the only one. These groups execute cyber-attacks against governmental and other enemy assets in cyberspace; they use propaganda to spread their ideological cause among they people. And, as we have noted, they organise simultaneous political protests in the physical world.

What, then, is the difference between hacktivism and cyber-insurgency? Traditionally, and as Galula also points out,[29] the line between political activism and insurgency has been very thin and vague. The shift from escalating activism to full-strength insurgency is usually gradual and hard to pin down. But the main difference relates to violence. Whereas activists and parties mostly hold rallies and protests and disseminate leaflets, insurgents instead focus on killing officials, ambushing armed forces and destroying infrastructure. To give some specific examples, the use and prevalence of violence are what distinguishes the Arab Spring in Tunisia from the Arab Spring in Libya. A second difference concerns insurgency's conspiratorial nature, which is partly a consequence of the violence on both sides of the conflict. Holding an open political rally becomes problematic when explosions and small arms fire are the order of the day.

But the concept of violence is very hard to translate into cyberspace. Violence is generally defined as the use of physical force with the purpose of harming someone or damaging something.[30] Using physical force in cyberspace is not possible because the domain is immaterial. Calling malware or specific cyber-attacks violent also constitutes a considerable inflation of the term; it offers no clear distinctions and, thus, seems wholly unproductive. Key questions remain: Are DDoS flood attacks exercises of physical force intending to damage something? Was Stuxnet violent?

It makes far more sense to follow the distinction that Denning makes when discussing cyber-terrorism.[31] This distinction is not about violence but instead based upon disruption and destruction. Hacktivism is disruptive: it blocks communication, substitutes and misappropriates content and circulates disparaging information. It inconveniences or annoys its victims. But cyber-terrorism and cyber-insurgency are – or

rather they would be – destructive. Factories might be damaged, traffic or power might be perpetually disabled and, if technology so allows, people might be killed. Distinctions along these lines better capture the nature of cyberspace. As such, they are more useful when researching cyber-threats than trying to copy the concept of violence directly over from physical space.

Given their common destructive and political nature, it may be tempting to equate cyber-insurgency with cyber-terrorism. But, in cyberspace, as in physical space, the two activities can be distinguished. As is often the case, the line is just not clear-cut. In their simplest and purest form, insurgencies attempts to win over or take control of the people while attacking and weakening the central authority. In contrast, terrorism can be described as a strategy for extorting concessions from the government by attacking the people themselves. The relationships within these two forms of conflict are, thus, slightly different. Terrorist attacks are meant to be violent and destructive spectacles which put pressure on their audience. The direct victims of the attacks are not that audience; they are just a means to induce fear in the real audience consisting of the rest of the population and the government. During an insurgency, in contrast, it is the people who are being fought over. This is why insurgent attacks usually target the government, the army and other mainstays of the central authority.

As Galula notes, these two approaches are not entirely mutually exclusive.[32] Terrorism may be useful for its shock value and ability to destabilise the state, and both these effects may also help insurgents to achieve their goals. This is true especially when insurgent action starts out very weakly, lacking a strong political cause that would rally the population alongside, or when government counter-insurgency efforts are overly strong and effective. Terrorism can grab headlines, achieve desired publicity for a cause and raise the political awareness of the population. Later on during the conflict, it may be used to maintain control of the population by staging public executions of "traitors," and thus, dividing the people from the government even further through fear. Still, for the most part, beyond its initial shock value, terrorism is detrimental to the insurgent cause. Protracted campaigns of fear alienate the population from a cause and can generate public support for counter-measures.

Applying these distinctions to cyberspace, we can expect cyber-terror attacks to be programmed for maximum shock value and fear with the intent of making central authorities yield to attackers' demands. Soft,

civilian targets would be the easiest to attack as they would generate maximum publicity when destroyed or killed. On the other hand, cyber-insurgency would involve attacking government systems, trying to destroy military, police and other institutional assets and assassinating select officials who represent the enemy or its regime.

We can pause here to distinguish cybercrime, which unlike all of the types of conflict discussed above, lacks an inherently political essence. This is quite straightforwardly what sets it apart from cyber-insurgency. Crime is carried out for profit and not for political goals, while cyber-insurgency is thoroughly political. Nevertheless, since in practice, groups or individuals can pursue both aims (and even seek to control the population in order to achieve them), the distinction can become somewhat blurry. After all, cyber-insurgents need money to expand and remain active, and organised crime organisations are easier to build and maintain if they manage to gain political influence (through corruption or blackmail, for example). Ultimately, however, while some overlap or cooperation may occur, the difference in the motives of profit-seeking criminals and politically motivated insurgents offers the clearest and most practical distinction between the two activities.

The last of the cyberspace activities set out above, cyber-espionage and cyber-sabotage do not themselves really constitute separate types of conflict. Rather, they serve as more specific (yet still quite broad) means of cyber-attack, independent of the overall aims of the actors who deploy them. As such, both can be used to full effect during all the listed types of conflicts and also linked to varying long-term goals.

In recent years, such attacks, especially when targeting state assets and systems, have followed a pattern which is the modern cyberspace equivalent of the traditional covert contest between different intelligence agencies and their proxies.[33] It would be problematic to describe these attacks, which are generally non-destructive (with the clear exception of Stuxnet), as "cyberwars" in the absence of an actual state of war or any armed clashes between the actors. Alternative names like "cyber-cold wars" may be more accurate. At the same time, they do not seem to add much conceptual content beyond what "cyberspace intelligence operations" in general and "cyber-espionage/sabotage" specifically already capture.

Why is Cyber-Insurgency Nowhere to Be Seen?

Having established the characteristics of cyber-insurgency and highlighted its distinguishing features, we have still to address the important

matter of its current absence. So, why is it that we do not see cyber-insurgency, as described above, on the world political scene?

The first reason why cyber-insurgency is missing comes almost directly from reflections on the similar case of cyber-terrorism, which is also notably absent. It stems from the necessarily destructive nature of both kinds of attacks. While cyber-terrorist attacks must cause harm in order to generate enough fear in their audience, cyber-insurgencies must be destructive to undermine state power, promote disorder, establish control over the people and thus exceed the merely disruptive nature of hacktivism. Currently, however, as we have seen, it remains relatively difficult to overcome the kinetic barrier and so achieve physically damaging outcomes through cyber-attacks.

This is especially true for non-state actors because they lack many of the resources along with the insider knowledge and dedication which allow some states and their agencies to push the boundaries of what can be achieved in this area. Insurgents are naturally non-state actors (unless they are being used as proxies and supported by another state). Therefore, it is not very likely that significant cyber-insurgency will take place before these kinds of attacks become more feasible. On the other hand, their feasibility might not be apparent until they actually start to happen.

The second reason for the absence of cyber-insurgency applies to cyber-warfare as well. As has been mentioned, in the absence of a modern inter-state war, there are few occasions when cyber-warfare may take place. Regions beset by conventional wars usually lack the infrastructure, appropriate targets and technical expertise needed to execute significant cyber-attacks that would support the on-going war in a noticeable way.

And similarly, while violent insurgencies have been occurring in those same regions, they are largely absent from the modern states dependent on the advanced and networked information systems which would provide fertile ground for cyber-attacks. Until states plagued by armed insurgencies are fully modernised, or those already modernised are embroiled in insurgent attacks, there will not be many opportunities for cyber-insurgency to take hold and develop. Assessing how probable these two scenarios are, or even which one of them is more likely, falls outside the scope of this study, however.

An alternative interpretation would call up the threat of "global cyber-insurgency." Consistent with the lack of national borders and territoriality in cyberspace, this would manifest in attacks spanning the globe and disregarding spatial proximity and distance. This trend is

already visible in hacktivism, especially when Western hackers support political conflicts in African or Asian states.

Things get more complicated when destructive attacks are considered because, as noted above, these – in some cases conventional – insurgencies take place in states which often lack the favourable conditions needed for their execution. Harmful cyber-attacks meant to undermine the power of a specific regime must almost certainly physically manifest themselves in aterritory which that regime controls. In other words, if a prospective cyber-insurgent living in Western Europe decides to help undermine a regime somewhere in Southwest Asia, then they must damage assets which are physically located in Asia, and not in Europe where the attacker lives. At least at present, this does not seem to be an easy task to accomplish.

The Preconditions for Insurgency

According to Galula, there are several prerequisites which must be met before insurgency can flourish.[34] The potential success or failure of an insurgency hinges largely on these preconditions. This should also hold true for cyber-insurgencies though, of course, with some modifications. Based on these prerequisites, we can also venture some observations about the likely nature of cyber-insurgency.

The first prerequisite relates to the cause behind the action. As has been noted, insurgents cannot succeed in gaining control of the population unless they represent and fight for a cause which both undermines the authority of the contested regime and attracts public support. A good cause is one whose validity the government cannot possibly accept, and which it cannot implement itself. Otherwise the insurgence will be drained of support before it even begins.

Any cause will invariably polarise the population and split it into three groups: those who support it; those who oppose it; and those who are passive or indifferent towards it. A protracted conflict will bring members of the last group to gradually align themselves with one of the extremes. Well-chosen causes attract the largest possible group of initial supporters, minimise opposition and lure those who have not yet had to decide. Later, the conflict will be intimately tied to the cause, rendering neutrality untenable.

Traditionally, insurgents picked their causes based on local politics and the local population. But, cyber-insurgency, as we have seen, opens up the conflict to a whole new set of actors who might decide to intervene

by making destructive attacks through cyberspace. Therefore, potential cyber-insurgents will need to consider how appealing their cause is to a wider audience. This was true to some degree even before the advent of cyberspace when volunteers would travel long distances to join the struggle they believed in. But in a cyber-insurgency, these volunteers do not even have to leave their homes and jobs. They can join in the fight while carrying on their regular lives, benefiting from the relative safety and anonymity that cyberspace provides.

This also means that the cause in question should call out especially to those who have the means to act upon it and can execute destructive cyber-attacks from outside. The highest concentration of such volunteers can probably be found in modern states characterised by the extensive use of information and communication technologies and corresponding education opportunities. The reason why the fight for freedom of information is such a popular cause among current hacktivists is that the people who are actually able to stage these attacks are the ones who find this cause personally appealing

The potential for external volunteers to have a significant impact on cyber-insurgencies is something that must be added to Galula's core conditions, particularly since he considers other states to be the only significant source of outside support. And there is another group of actors who might influence cyber-insurgencies: private companies. They carry out much of the technical development, run the infrastructure and also supply both hardware and software which are used to operate and even protect critical assets. Their attitude to the cause could prove decisive when insurgents seek to carry out destructive cyber-attacks and when counter-insurgent forces try to thwart their success. Obtaining their support and avoiding their opposition should therefore be goals which both sides consider pursuing in a cyber-insurgent conflict.

Geography also plays a crucial role here. Translating this into the cyber-insurgency context is problematic, however, because of the different nature of space itself in this domain. There is, of course, no physical geography to speak of in cyberspace; there are no mountain ranges or deserts. Some aspects of geography – climate, economic development levels, population density, for example – have no meaning in this realm. This is largely because much of cyberspace is uniformly accessible from anywhere and free of any limits. Frequently visited and economically thriving areas occupy the same space as abandoned and destitute ones.

Geography partitions the land and makes some areas more difficult to access than others in a conventional insurgency. But there are some comparatively inaccessible areas of cyberspace too. They are the equivalents of mountains and rivers, but are all man-made. A very prominent example is the national filtering done by governments in an attempt to prevent local populations from accessing "undesirable" content. Following a similar principle, but on a smaller scale, protected local area networks are supposed to prevent attackers and malware from coming in from the outside. Virtual private networks are another example of this "cyber-geography." They enable a more secure exchange of information between endpoints, thus circumventing much filtering. These features can be considered the cyberspace equivalents of rivers and fords – or perhaps given their artificial nature, fortifications and tunnels may be a more appropriate analogy.[35]

Another major area of cyberspace with altered accessibility and visibility is the Deep Web, which is sometimes also called the Darknet. This is a network of hidden servers, anonymised services and encrypted information flows not reachable by regular means. This area is the cyberspace equivalent of mountain ranges and jungle, and it is next to impossible to observe what is happening inside it. It remains largely beyond the reach of regulation. Unsurprisingly, it is already providing a haven to both criminals and political dissidents.[36]

The most extreme form of geography in cyberspace is the complete physical separation of networks. Such a separation (also called an air-gap) theoretically prevents any malware or direct hacking attack from reaching its target over the Internet, and it is how the most sensitive systems are protected. Air-gaps open up a veritable ocean or chasm in cyberspace whose crossing requires entry into another domain. But whereas real oceans and chasms can be crossed by leaving land and travelling by air or sea, the cyberspace equivalent must be traversed through a physical domain. In practice, this elaborate analogy usually boils down to someone physically carrying malware over the gap via their USB flash drive or another portable data storage device.[37]

The last of Galula's prerequisites for an insurgency is the weakness of the opponent. This weakness is closely connected to the political cause discussed earlier and mostly describes the regime's inability to react efficiently to the threat posed by nascent insurgency. Issues like a weak political structure, internal fractures or incompetent security

forces make the job of insurgents easier. This applies to insurgencies conducted in physical space as well as those in cyberspace, and there is little conceptual difference between the two.

One of the informing ideas of the first part of this study was the mounting of simultaneous action in cyberspace and physical space. This tactic is especially important during cyber-warfare and hacktivism, but mostly absent from cybercrime and cyber-espionage. This is mainly because of the covert nature of the latter activities. The long-term success of both crime and espionage operations largely depends on their target not knowing it is under attack. It is significantly more difficult to fool a victim if it knows it is being deceived. Obscurity and a lack of physically apparent consequences are therefore critical to these attacks' successful continuation.

On the other hand, war and political activism are already apparent and visible to everyone. They can hardly be conducted without actions happening in the physical world such as leaders making demands, crowds gathering in the streets and military hardware moving around. Under these conditions, it would generally only be an advantage to take concurrent actions in cyberspace that boost offline efforts. These actions could include defacing news portals with one's own message, hacking into opponents' databases to look for information or even taking an enemy power grid offline.

In an active cyber-insurgency, attackers would also benefit from supporting their physical operations with same-time attacks in cyberspace. These strikes could delay the reactions of counter-insurgent forces, hinder their movements, weaken their response or stretch their resources by causing damage and deaths in multiple locations at the same time. In this respect, cyber-insurgency probably comes closer to cyber-warfare than to cyber-espionage.[38]

Clearly, different actors strive to conceal or publicise their attacks to different degrees. As we have seen, some strikes are supposed to remain concealed for as long as possible while others are meant to attract attention. Hacktivism especially seeks out attention and often goes so far as to publicly announce a target even before it is attacked.

More commonly, cyber-attacks are planned and executed in secret. But once an attack (or even a series of attacks) is complete, its results are widely publicised to achieve the maximum impact on the audience. The same pattern can be expected from cyber-insurgencies given their

focus on the population. But this is hardly surprising and quite analogous to how publicity is already handled during conventional insurgencies in physical space. This attention-seeking behaviour is definitely not exclusive to cyberspace; it is simply made easier there.[39]

Conclusion

Cyber-insurgency is still a hypothetical situation. Nevertheless, it is sufficiently distinctive from other forms of conflict to stand its own ground. Unlike cybercrime, its goals are political and not profit-oriented. Unlike cyber-warfare, it is highly asymmetrical and involves controlling the population. It follows the logic of hacktivism, but whereas hacktivism is essentially disruptive, cyber-insurgent attacks would be far more severe, destructive and lethal. It also differs from cyber-terrorism since it focuses on attacking and disrupting a regime rather than extorting and intimidating its people.

The absence of cyber-insurgency to date can mostly be ascribed to the lack of conducive political conflicts in states with sufficiently developed information infrastructure and integrated networked systems. Breaking through the kinetic barrier – that is, achieving significant physical destruction solely through a cyber-attack – also remains a major hurdle, especially for non-state actors. It remains to be seen where the first genuine cyber-insurgency will erupt and for what cause. Nor can we say when the first truly destructive and potentially even lethal political cyber-attack will strike. It could be months or decades away.

An additional benefit of studying cyber-insurgency's potential emergence is that it highlights interesting parallels between physical space and cyberspace along with their substantial differences. The transformation of society and civilisation which was triggered by the expansion of cyberspace is on-going and not yet fully understood. By looking forward and realistically anticipating the potential impact of cyberspace on our conflicts, we can avoid being caught unawares by sudden developments.

JAKUB DRMOLA is affiliated to the Department of Political Science of Masaryk University in Brno. He may be reached at:
jdrmola@mail.muni.cz

This work was created as part of 'Elections, parties and pursuit of interests II,' a research project of the Department of Political Science of FSS MU (code MUNI/A/0846/2013).

Notes

1. David Galula (1964), *Counterinsurgency Warfare: Theory and Practice*, New York: Praeger, p.104, available at: <http://armyrotc.missouri.edu/pdfs-docs/Galula%20David%20-%20Counterinsurgency%20Warfare.pdf> (accessed 27 January 2014).
2. See Umer Asgher, Fahad Moazzam Dar, Ali Hamza and Abdul Moeed Paracha (2013), 'Analysis of Increasing Malwares and Cyber Crimes Using Economic Approach,' *The International Journal of Soft Computing and Software Engineering* Vol. 3, No. 3, pp. 487-491, available at: <http://arxiv.org/ftp/arxiv/papers/1401/1401.5178.pdf>, or United Nations Office on Drugs and Crime (2010), 'Cybercrime,' available at: <http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf> (accessed 27 January 2014).
3. Timothy B. Lee (2012), 'As Anonymous Protests, Internet Drowns in Inaccurate Anti-ACTA Arguments,' *Ars Technica*, 30 January, available at: <http://arstechnica.com/tech-policy/2012/01/internet-awash-in-inaccurate-anti-acta-arguments/> (accessed 27 January 2014).
4. D.C. Elliott (2009), 'Anonymous Rising,' *LINQ,* Vol. 36, pp. 96-111, available at: <http://www.linq.org.au/wp-content/uploads/LINQ-Vol-36.pdf> (accessed 27 January 2014).
5. Sean Captain (2011), 'The Real Role of Anonymous in Occupy Wall Street,' *Fast Company,* available at: <http://www.fastcompany.com/1788397/real-role-anonymous-occupy-wall-street> (accessed 27 January 2014).
6. Shyamantha Asokan (2011), 'The "Hacktivists" of Telecomix Lend a Hand to the Arab Spring,' *The Washington Post,* 07 December, available at: <http://www.washingtonpost.com/lifestyle/style/the-hacktivists-of-telecomix-lend-a-hand-to-the-arab-spring/2011/12/05/gIQAAOsraO_story.html> (accessed 27 January 2014).
7. The other four domains are (in chronological order of their becoming accessible) land, sea, air and outer space. Cyberspace is, thus, the most recent addition to the list. See William J. Lynn III (2010), 'Defending a New Domain,' *Foreign Affairs,* Vol. 89, No. 5, pp. 97-108.
8. For a list of wars in the period 1816 - 2007, see the Correlates of War (2010) data set: <http://www.correlatesofwar.org/COW2%20Data/WarData_NEW/WarList_NEW.pdf> (accessed 27 January 2014).
9. David M. Hollis (2011), 'Cyberwar Case Study: Georgia 2008,' *Small Wars Journal*, available at: <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008> (accessed 27 January 2014).
10. Comparing their usefulness in military conflict suggests that the two domains (i.e. space and cyberspace) are both well-suited for collecting in-

formation on the enemy. However, while space-based systems can also efficiently distribute information to friendly forces and provide communication channels, current cyber-warfare tools are generally more geared to disrupting information flows within enemy systems and shutting down unwanted communication channels. The two domains are, in a sense, complementary.

11. Erik Gartzke (2012), 'The Myth of Cyberwar,' *International Security,* Vol. 38, No. 2, pp. 41-73, available at: <http://dss.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf> (accessed 27 January 2014).
12. Nicolas Falliere, Liam O Murchu and Eric Chien (Symantec Security Response) (2011), *W32.Stuxnet Dossier*, white paper, Cupertino: Symantec Corporation, available at: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> (accessed 27 January 2014).
13. Stuxnet is not the only claimed case of a cyber-attack with physical consequences. Very widely mentioned is the case of the Siberian gas pipeline explosion caused by a "logic bomb" planted by the CIA during the Cold War. Unfortunately, every single allusion to this event can be traced back to a single original source (a memoir by Thomas C. Reed), which has never been supported by material evidence or independent confirmation. For a comparison, see Gus W. Weiss (2008), 'The Farewell Dossier,' *Studies in Intelligence*, available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm> (accessed 27 January 2014).
    Less well-known is the alleged cyber-assassination of a hospitalised "mob boss" in Italy. This allegation also has only one source - this time a Nigerian newspaper report: see 'Cyber Terrorism Hits Nigeria,' (2010), *Daily Sun*, September 25, available at: <http://newafricanpress.com/2010/09/25/cyber-terrorism-hits-nigeria/> (accessed 27 January 2014). Much of the limited publicity that this story received arose from a post at DefenseTech.org which cited the original article as "evidence": Kevin Coleman (2010), 'A Cyber Assassination Confirmed?' *DefenseTech,* September 29, available at: <http://defensetech.org/2010/09/29/a-cyber-assassination-confirmed/> (accessed 27 January 2014).
    A final example comes from the Polish town of Lodz where a schoolboy managed to assemble an infrared remote control for shifting tram tracks in 2008. This resulted in the derailment of a tram and several minor injuries: see Graeme Baker (2008), 'Schoolboy Hacks into City's Tram System,' *The Telegraph*, 11 January, available at: <http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html> (accessed 27 January 2014). Though it exposed exploitable deficiencies in the public transportation system, this was basically a juvenile prank with very little political or military significance.
    Ultimately, none of these events (whether real or fictitious) offers much insight into political conflicts in cyberspace.
14. Alexander Gostev (2012), 'The Flame: Questions and Answers,' *Securelist* (blog), May 28, available at: <http://www.securelist.com/en/blog?we-

blogid=208193522> (accessed 27 January 2014).
15. Symantec Security Response (2011), *W32.Duqu: The Precursor to the Next Stuxnet*, white paper, Cupertino: Symantec Corporation, available at: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf> (accessed 27 January 2014).
16. Kaspersky Labs' Global Research & Analysis Team (2013), *"Red October" Diplomatic Cyber Attacks Investigation*, available at: <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation> (accessed 27 January 2014).
17. United Nations Office on Drugs and Crime (2012), 'The Use of the Internet for Terrorist Purposes,' available at: <http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> (accessed 27 January 2014).
18. Dorothy Denning (2011), 'Whither Cyber Terror?', in *10 Years After September 11: A Social Science Research Council Essay Forum*, available at: <http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/> (accessed 27 January 2014).
19. Dorothy Denning (2009), 'Barriers to Entry: Are They Lower for Cyber Warfare?' *10 Journal,* April 2009, available at: <http://faculty.nps.edu/dedennin/publications/Denning-BarriersToEntry.pdf> (accessed 27 January 2014).
20. Dorothy Denning (2001), 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,' in J. Arquilla and D. F. Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND Corporation, pp. 239-288, available at: <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf> (accessed 27 January 2014).
21. Timothy L. Thomas (2006), 'Cyber Mobilization: A Growing Counterinsurgency Campaign,' *10 Sphere,* Joint Information Operations Center, Summer 2006, pp. 23-28, available at: <http://fmso.leavenworth.army.mil/documents/cyber-mobilization.pdf> (accessed 27 January 2014).
22. Paul Rosenzweig (2013), *Cyber Warfare,* Santa Barbara: Praeger, pp. 59-66.
23. Samuel Liles (2010), 'Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency,' in C. Czosseck and K. Podins (eds.), *Conference on Cyber Conflict, Proceedings 2010,* Tallin, Estonia: CCD COE Publications, , available at: <http://www.ccdcoe.org/publications/2010proceedings/Liles%20-%20Cyber%20warfare%20%20As%20a%20form%20of%20low-intensity%20conflict%20and%20insurgency.pdf> (accessed 27 January 2014).
24. The current US Army counter-insurgency field manual cites Galula frequently; see 'Counterinsurgency,' FM 3-24, Headquarters, Department of the Army, available at: <http://www.fas.org/irp/doddir/army/fm3-24.pdf> (accessed 27 January 2014).
25. Jeremy Fordham (2011), 'Another Look at Entropy,' *Understanding Uncertainty* (blog), available at: <http://understandinguncertainty.org/another-look-entropy> (accessed 27 January 2014).
26. See Stephen Graham (1998), 'The End of Geography or the Explosion of

Place? Conceptualizing Space, Place and Information Technology,' *Progress in Human Geography,* 22-2, pp. 165-185, available at: <http://www.realtech-support.org/UB/NP/IoT_ExplosionSpace_1998.pdf> (accessed 27 January 2014).

27. This may, of course, change in the future. Technological advances and changing environments may make concepts like flying cities, floating cities and large and populous space stations a feasible and desirable reality. If this comes to pass, it is quite likely that there will be insurgencies in these habitats as well. This is not an issue for the near future, however, and it falls outside the scope of this study.
28. Balaji Srinivasan (2013), 'Software is Reorganizing the World,' *Wired*, 22 November, available at: <http://www.wired.com/opinion/2013/11/software-is-reorganizing-the-world-and-cloud-formations-could-lead-to-physical-nations/> (accessed 27 January 2014).
29. Galula (1964), pp. 7-8.
30. See the dictionary entries for "violence" at Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/violence; Oxford English Dictionary, http://www.oxforddictionaries.com/definition/english/violence?q=violence.
31. Denning (2001), pp. 24-26.
32. Galula (1964), pp. 43-46.
33. Mandiant (2013), 'APT1: Exposing One of China's Cyber Espionage Units,' available at: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf> (accessed 27 January 2014).
34. Galula (1964), pp. 13-31.
35. Thomas J. Pingel (2003), 'Key Defensive Terrain in Cyberspace: A Geographic Perspective,' in *Proceedings of the 2003 International Conference on Politics and Information Systems: Technologies and Applications*, Orlando, FL, pp. 159-63, available at: <http://www.academia.edu/4539134/Key_Defensive_Terrain_in_Cyberspace_A_Geographic_Perspective> (accessed 27 January 2014).
36. Clive Thompson (2013), 'The Darkest Place on the Internet Isn't Just for Criminals,' *Wired,* 18 October, available at: <http://www.wired.com/opinion/2013/10/thompson/> (accessed 27 January 2014).
37. Bruce Schneier (2013), 'Want to Evade NSA Spying? Don't Connect to the Internet,' *Wired,* 07 October, available at: <http://www.wired.com/opinion/2013/10/149481/> (accessed 27 January 2014).
38. This may also be true of cyber-terrorism, i.e. it may be more like cyber-warfare than cyber-espionage.
39. Dorothy Denning (2011), 'Cyber Conflict as an Emergent Social Phenomenon,' in T. Hold and B. Schell (eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, IGI Global, available at: <http://faculty.nps.edu/dedennin/publications/CyberConflict-EmergentSocialPhenomenon-final.pdf> (accessed 27 January 2014).