**Cyber-bombing Dresden: attacks on internet infrastructure and international humanitarian law**

|  |
| --- |
| Two states, the Republic of Possible and the Commonwealth of Hypothetica, are in a state of conflict. Possible, by cyber and/or physical means, launches an attack on Hypothetica, the effect of which is to disable essential internet services, or otherwise cripple Hypothetica's internet infrastructure to the point where Hypothetica is "disconnected".  This paper does not discuss why the states are at conflict. It is of practical irrelevance to consider the how and why of the events leading up to this point. Instead, the object of this paper is to consider whether Possible has, by its disabling of Hypothetica's internet infrastructure, inflicted harm on Hypothetica's civilian population to the extent that Possible has breached the protections granted to civilians in conflict under international humanitarian law. |

**Introduction**

In February 1945, the United States Army Air Force, as it then was, bombed the city of Dresden, causing a firestorm that destroyed much of the city and resulted in an estimated 25,000 casualties.[[1]](#footnote-2) While Dresden certainly had value as a military target, it has also been questioned whether the attack was necessary or proportionate to its military value with respect to the massive destruction and detriment to the civilian population, particularly at this late stage of the war, and the legality of the bombing has been debated at length ever since. Supporters have justified the bombing on the basis that a number of factories and military units were based in and around the city at the time, making the city a legitimate military target. Detractors have questioned the necessity of the attack on the basis that the military value of the city as a target was overestimated, or decried the indiscriminate nature of the attack and the likelihood of civilian suffering (Dresden playing host to several hundred thousand refugees fleeing from the Red Army at the time).

In modern conflicts, a distinction between objects of a military nature and objects of a civilian nature has generally been recognised. While civilian objects may have been targeted during a conflict (deliberately, in order to demoralise the civilian population as part of the 'hearts and minds' campaign, or accidentally or indiscriminately in pursuit of a direct military objective), during the last century, and particularly since Nuremberg, developed states have generally attempted as a matter of policy or under what is now called international humanitarian law to limit the targets of attack to reduce the risk to civilian objects and the harm done to the civilian population.[[2]](#footnote-3)

International humanitarian law regarding the treatment of civilians during conflict is now well established. For example, Article 51 of Protocol I to the Geneva Conventions (**Article 51)** provides a number of broad terms with the aim of generally protecting civilians and civilian objects from unnecessary or indiscriminate danger or attack during a military conflict (emphasis added):

1. The civilian population and individual civilians **shall enjoy general protection against dangers arising from military operations.** To give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances.
2. The **civilian population** as such, as well as individual civilians, **shall not be the subject of attack.** Acts or theatres of violence the **primary purpose of which is to spread terror** among the civilian population **are prohibited**.
3. Civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in hostilities.
4. **Indiscriminate attacks are prohibited**. Indiscriminate attacks are: (a) those which are **not directed at a specific military objective**; (b) those which employ a **method or means of combat which cannot be directed at a specific military objective**; or (c) those which **employ a method or means of combat the effects of which cannot be limited** as required by this protocol;

and consequently, in each such case, are **of a nature to strike military objectives and civilians or civilian objects without distinction**.

1. Among others, the following types of attacks are to be considered as indiscriminate: (a) an attack by bombardment by any methods or means which **treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects**; and (b) an attack which may be **expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive** in relation to the concrete and direct military advantage anticipated.
2. Attacks against the civilian population or civilians by way of reprisals are prohibited.
3. The presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations. The Parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations.
4. Any violation of these prohibitions shall not release the Parties to the conflict from their legal obligations with respect to the civilian population and civilians, including the obligation to take the precautionary measures provided for in Article 57.

The distinction between military and civilian objects contemplated by Article 51, and international humanitarian law generally, arises from the historical reality that that most tangible objects are usually dedicated predominantly to an exclusively civilian or an exclusively military purpose. Factories are unlikely to produce tanks and toasters alongside each other. Those objects recognised as essential or otherwise of significance to the civilian population (e.g. fields and agriculture,[[3]](#footnote-4) water supplies,[[4]](#footnote-5) religious and cultural structures,[[5]](#footnote-6) and other objects required for physical or mental sustenance)[[6]](#footnote-7) have been acknowledged as possessing a special status under international humanitarian law protecting them from attack unless such attack is militarily justified. Attacks intended to cause terror or other suffering generally to civilians, or which indiscriminately target civilian and military objects alike, are also prohibited.

However, proliferate adoption of the internet across the developed world has blurred the lines between “military” and “civilian” objects and purposes to a greater extent than any human creation before it. The internet has, to some extent, become indispensable for ordinary life in many countries. In addition to the cultural and social influence of the internet, many services essential for civilian life (including commerce and government services) now either operate over the internet or are built on internet-based infrastructure. However, the internet also has undeniable and similarly proliferate military applications, making the internet (or parts thereof) legitimate military targets in the event of a conflict.

For a developed state, a military attack on its internet infrastructure with the effect of disabling or crippling the state's internet capability may be devastating. Trade and commerce within and beyond the borders of the country under attack may grind to a halt. Government services may be limited. Ordinary people may be unable to go about the usual social and cultural activities they currently enjoy (insofar as Facebook or Youtube can be considered a social or cultural activity). Worse, essential services are increasingly linked via internet infrastructure, suggesting that injury or death may occur if, for example, medical information hosted online became inaccessible to hospitals, or internet-enabled control over utilities or major installations were lost. Of course, it is possible that some services may be unaffected while some rendered unusable, though it may be scant comfort that Facebook and Youtube remain accessible while health records are corrupted and public utilities become uncontrollable (even the most addicted person would be likely to wish for a reversal in time).

Despite this, academic consideration of attacks on internet infrastructure has generally focused on the *jus in bello* question of whether an electronic, or “cyber”, attack constitutes an act of war. There has been comparatively less consideration of the *jus ad bellum* question of whether the consequences of such attack may be in breach of international humanitarian law. I propose to consider whether an attack on a states' internet infrastructure is a breach of international humanitarian law, specifically a breach of Article 51, and determine at what point such an attack may lose focus of its military objectives to the extent that the attack becomes indiscriminate of military and civilian internet objects: or in other words, cyber-bombing Dresden.

While it is impossible to consider every factor which may apply to such a scenario, using the imaginary states of the Republic of Possible and the Commonwealth of Hypothetica, I will consider a single, simple question:

**If Possible attacks Hypothetica's internet infrastructure, and Hypothetica subsequently loses critical internet services or the internet generally is crippled to the point that the it is rendered unusable by Hypothetica's citizens, is Possible in breach of Article 51 of Protocol I to the Geneva Conventions?**

In **Part I** of this paper, I consider the internet as an object under international humanitarian law:

1. The internet is susceptible to both electronic and physical attacks. It is appropriate to consider how such attacks have been considered previously in academic literature and how the internet has been threatened in states in conflict in the past, and from this consider how to define an attack on internet infrastructure for the purpose of this paper.
2. There are many uses of the internet, and an attack on internet infrastructure may be considered under multiple articles of international humanitarian law. However, as above, I will consider attacks on internet infrastructure in light of Article 51, and propose that the broad scope of this article as compared to other articles of international humanitarian law makes it the most appropriate to consider with respect to attacks on internet infrastructure.

In **Part II** of this paper, I consider the multiple methods of attack in light of Article 51:

1. Electronic, or “cyber”, attacks are effective means of attack, but are relatively difficult to target. To some extent, the acts required to increase the likelihood of a successful attack also increase the likelihood that the attack will breach Article 51.
2. Physical attacks on internet infrastructure within a target state's borders may theoretically be targeted at infrastructure dedicated to military purposes. However, the nature of the internet suggests that use of internet infrastructure in this way is uncommon and that such an attack will have civilian consequences.
3. Physical attacks on internet infrastructure outside the target's state may or may not cause detriment to the civilian population depending on the geographical location and level of development of the target state. The more likely that there is a military benefit to the attack goes hand-in-hand with the likelihood that there will be significant civilian consequences.

Finally, in **Part III** of this paper, I will consider whether international humanitarian law is capable of accommodating attacks on internet infrastructure:

1. International humanitarian law is traditionally focused on preventing unnecessary civilian injury or loss of life, or damage to civilian objects. However, an attack on internet infrastructure may result in damage which does not fall under any of these categories but nonetheless has severe consequences for the life of the civilian population. It is difficult to reconcile these positions.
2. It has been proposed that attacks on internet infrastructure be recognised in international humanitarian law, the same way that firebombing was recognised after World War II. However, I suggest that there is substantial difficulty in finding a definition of such attacks which is likely to be acceptable to the international community, particularly as any definition has the obvious risk of becoming out-of-date with regards to technological development.
3. International humanitarian law is not a criminal code, but a regulation of warfare which has been accepted by the international community. I propose that despite its flaws with regard to attacks on internet infrastructure, international humanitarian law still succeeds not as a method of punishment, but as a method of deterrence.

**Part I: The Internet under International Humanitarian Law**

While actual observation of the principle has come and gone throughout history, the general principle that civilians should not be the focus of deliberate or indiscriminate attack has persisted and been recognised by most belligerents of an established nature (i.e. recognised state actors) in modern history.[[7]](#footnote-8) However, it is a mistake to suggest that civilians are protected absolutely from any form of hardship during a conflict. Even in the absence of any overt enemy military activity, the civilian population will suffer, to some extent, due to the diversion of resources to support the conflict and disruption to services and lifestyle.[[8]](#footnote-9)

The purpose of international humanitarian law is not to shield civilians totally from conflict, but to excuse them from direct threat solely for the purpose of causing harm to the civilian population.[[9]](#footnote-10) Of course, as war has changed, international humanitarian law must also adapt in light of the weapons of the day: modern weapons allow destruction both indiscriminate and widespread that would have been unimaginable in the days of sword, or musket and shot. Similarly, firebombing specifically was outside the contemplation of international humanitarian law until after World War II, during which it had been used by most belligerents.[[10]](#footnote-11)

However, the internet does not fall neatly into international humanitarian law as it has developed thus far. The internet is an indisputably valuable military resource, and subsequently a military target of significant worth. Unfortunately, the same factors that make it an invaluable military object also render it an invaluable civilian object. Rarely has a method of attack been capable of striking both military and civilian targets to the same extent in the same blow.

**I (a): Technological infrastructure attacks**

It is indisputable that disabling the internet of a country may result in significant advantages on the battlefield or otherwise in the conduct of a conflict, but such an attack may arguably also cause such suffering across the target's civilian population that the cost of the attack outweighs the military advantage gained. Like any other attack, military planners must consider the likelihood of civilian casualties or suffering against the direct military benefit.

The concept of attacking the internet infrastructure of a state in order to disrupt the activities of that state is not merely hypothetical, and the effect of a widespread loss of internet connectivity to an industrialised country has been well established:

1. In 2007, cyber-attacks against Estonia brought down major internet services and crippled the internet in the country to the extent that the internet was unusable. In Estonia, everything from banking to taxes to parliamentary elections are carried out online, and e-payments are considered standard, enabled by proliferate wi-fi availability. For a country so heavily dependent on the internet to function, such an attack effectively brought civilian life in the country to its knees.[[11]](#footnote-12)
2. In 2008, a cyber-attack on Georgia coinciding with the Russian occupation of the separatist South Ossetian region of Georgia brought Georgian internet to a halt, with Georgians struggling to communicate with each other within their borders and all but unable to communicate with the rest of the world.[[12]](#footnote-13)

With respect to the vulnerability of internet infrastructure, and technological infrastructure generally, the bulk of the current academic literature has focused on purely electronic or “cyber” attacks. While this approach is certainly worthwhile, it is somewhat lacking as the vulnerability of physical technological infrastructure is overlooked entirely. This approach is also lacking with respect to the *jus ad bellum* question, as we are not concerned with the method of attack as such, but the consequences of the attack from the perspective of the civilian population.

In order to adequately consider possible breaches of international humanitarian law, both electronic and physical attacks must be considered. The internet of a state may be disabled or crippled by physical interference or destruction of the physical nodes and telecommunications cables through which it operates as effectively as an electronic attack through a computer network. We are not concerned with *how* the internet has been disabled; we are concerned that the internet *has* been disabled. This approach is consistent with consideration of international humanitarian law generally with respect to the protection of civilians: while the method of attack requires fresh consideration of the existing principles, the law has generally focused on the outcome of an attack rather than questioning the method by which the attack is made, e.g. an unlawful reprisal against a civilian population is an unlawful reprisal whatever the means.

If both electronic and physical methods of attacking internet infrastructure are to be considered, some definition must be provided to encapsulate those methods of attack under consideration. Hathaway and Crootof propose a promising definition of “cyber-attack” which may encompass all means by which the internet may be attacked:

“A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.”[[13]](#footnote-14)

This definition is initially promising, as it considers any action, which may encompass physical attack as much as electronic attack. However, at least for Hathaway and Crootof, the cyber attack remains an electronic attack, which leaves this definition as something of a mixed blessing in the context of their discussion. Further, the term “cyber attack” itself is a loaded term, as it is generally interpreted as meaning some attack by electronic means, making it difficult to redefine.

For need of a better term, in this paper I have adopted the term **technological infrastructure attack**, with acknowledgement to Hathaway and Crootof:

A technological infrastructure attack consists of any action by a state, by physical or electronic means or otherwise, to undermine the functions of the internet of another state.

Technological infrastructure attacks are not, in and of themselves, of specific concern under international humanitarian law. There is no reason to suggest that a legitimate military target is or should be immune to cyber-attack, or should be immune to attack (by any means) if the target is of an intangible technological nature.[[14]](#footnote-15) The difficulty arises where considering the requirements of distinction between military and civilian targets and proportionality between the effects on the civilian population and the military benefit.

**I (b): Article 51**

While technological infrastructure attacks may, and should, be considered under many sources of law, as a matter of practicality I must limit this paper to one particular article of international humanitarian law. For the purpose of this paper, I will be considering technological infrastructure attacks with respect to Article 51 (emphasis added):

1. The civilian population and individual civilians **shall enjoy general protection against dangers arising from military operations.** To give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances.
2. The **civilian population** as such, as well as individual civilians, **shall not be the subject of attack.** Acts or theatres of violence the **primary purpose of which is to spread terror** among the civilian population **are prohibited**.
3. Civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in hostilities.
4. **Indiscriminate attacks are prohibited**. Indiscriminate attacks are: (a) those which are **not directed at a specific military objective**; (b) those which employ a **method or means of combat which cannot be directed at a specific military objective**; or (c) those which **employ a method or means of combat the effects of which cannot be limited** as required by this protocol;

and consequently, in each such case, are **of a nature to strike military objectives and civilians or civilian objects without distinction**.

1. Among others, the following types of attacks are to be considered as indiscriminate: (a) an attack by bombardment by any methods or means which **treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects**; and (b) an attack which may be **expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive** in relation to the concrete and direct military advantage anticipated.
2. Attacks against the civilian population or civilians by way of reprisals are prohibited.
3. The presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations. The Parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations.
4. Any violation of these prohibitions shall not release the Parties to the conflict from their legal obligations with respect to the civilian population and civilians, including the obligation to take the precautionary measures provided for in Article 57.

I propose that Article 51 is the most appropriate article of international humanitarian law to consider in the context of a technological infrastructure attack as, unlike many other articles, Article 51 espouses a broad and general principle that the civilian population and civilian objects should be shielded from attack, whether that attack is deliberately targeted towards the civilian population or civilian objects, or whether the damage is done as a result of an indiscriminate attack. By comparison, other articles are somewhat more limited in scope, protecting only specific objects, e.g. Article 54 prohibits attack on objects essential to the survival of the civilian population (non-exhaustively defined as foodstuffs, agricultural areas, livestocks, and water installations), and Article 56 prohibits attack on installations containing dangerous forces (defined as dams, dykes and nuclear power stations).

A reasonable interpretation of Article 51 would encompass all these and other civilian objects (assuming a civilian application of the objects) under the general umbrella term of “civilian objects”, and may also be protected under the more general principle that civilians should not be subject to attacks of terror, or be placed in danger. In this respect, Article 51 has a lower threshold requirement: it is not necessary to prove that the object of attack was a particular class of object (although it may be useful to do so in order to qualify the outcome for the civilian population), only that the attack exposed the civilian population to some danger in excess of the comparative military value of the attack and within the ordinary course of conflict.

**II: Legality of technological infrastructure attacks under Article 51**

Nothing about technological infrastructure attacks as a new means of attack detract from the general principle established in Article 51(4) that attacks which are uncontrollable or indiscriminate are prohibited. Nor is any question raised where the distinction between a military and a civilian object is clear: an attack specifically against and limited to a military target will not be in breach of Article 51, and similarly, an attack specifically against a dedicated civilian object will almost certainly be in breach of Article 51. The fact that the objects may consist of internet infrastructure is irrelevant to the extent that such scenarios apply.[[15]](#footnote-16) The greater difficulty comes in balancing the issue of the internet generally as both a civilian and military object, and the complexity of attacks against internet infrastructure and the subsequently increased likelihood that such attacks may be indiscriminate in practice if not intent.

For the purpose of this paper it should be sufficient, as should be well established in common knowledge, that the internet (defined simply) is a network of computers between which data (i.e. computer files) may be transferred and shared.

It is often claimed that the internet was designed to be sufficiently robust, through the untold number of connections between computers, that it could survive nuclear war. While this idea of robustness is theoretically true, in practice the internet is dependent on a number of "backbone" links. For example, all but a small percentage of international internet traffic in Australia is routed through a handful of major undersea telecommunications cables running between major Australian cities and other cities on the western seaboard of the United States, and to a lesser extent in south-east Asia. A similar backbone exists between major cities. Eliminating any of these connections, or any of the 'nodes' on the network, may result in major issues.

While I am interested in the outcome of an attack rather than the method thereof, the methods of attack must be understood, if only generally, when considering the comparative ability of a technological infrastructure attack to be focused towards a particular target and the implications with respect to proportionality and discrimination between targets.

Formally under international humanitarian law, a civilian presence does not necessarily render a legitimately military target immune from attack. Particularly, a state is not allowed to use a civilian presence as a shield, or place civilians under threat of attack as a shield. However, while this may be very true for physical facilities where a civilian and military presence may come and go from time to time, the internet is a single object common to both civilian and military at all times. In order to avoid complications under international humanitarian law, any aggressor must therefore ensure that any attack is limited, to the greatest extent possible, to the military attributes of the technological infrastructure.

In the context of our belligerents, Possible may cripple Hypothetica's internet infrastructure, perhaps to the extent where the internet becomes unusable to Hypothetica's population, via:

1. a remote electronic or “cyber” attack over a computer network;
2. a direct attack on physical infrastructure within Possible; or
3. a direct attack on physical infrastructure outside Hypothetica's borders.

**II (a): What if Possible uses its own computers in a remote electronic (“cyber”) attack to disable computers in Hypothetica7?**

Whenever the concept of “attacking the internet” or a similar concept is raised, a Hollywood-esque scenario comes to mind: a single person, or team of people, using advanced computer skills in order to disable or otherwise manipulate the computer of a target person, organisation or country. The perpetrators of such attacks may be criminals, states, or Matthew Broderick.

In theory, an electronic technological infrastructure attack may be a precise instrument of conflict, and has been used for “precision” attacks in the past. In the absence of a specific vulnerability leaving the target computer system open to attack, the most common method of attack is a “denial-of-service” attack.

In a denial-of-service attack, the attacker sends fake traffic to the target with the intention of either overloading the target’s internet connection, or causing the target’s hardware to fail due to excessive stress. If the target computer system and internet connection are analogous to a car park and road network, an attacker may send many cars to fill up the spaces at the targeted car park, denying others the ability to use that car park. Even if not enough cars are sent, the attack places many more cars on the road, possibly so many that the entire road network around the car park shuts down due to congestion. Either way, the target has been successfully neutralised.

While denial-of-service attacks may be effective, they may also be indiscriminate: excessive network traffic will result in network slowdowns for anyone relying on those networks, not just the target of the attack, and it also may not be possible to predict whether there will be any collateral loss (e.g. if a state's Department of Defence internet infrastructure was hosted in the same data centre as that state's health services, and that data centre became the object of attack, both defence and health services would be affected). These issues are exacerbated by the nature of denial-of-service attacks: the more fake traffic is sent the greater the probability the attack will be successful, so the attacker has a vested interest in sending far more fake traffic than technically necessary, consequently resulting in a greater risk of cascading failure across multiple services.

In the context of Article 51, electronic attacks risk breaching the prohibition against indiscriminate attack and attacks which may be expected to cause incidental damage to civilian objects excessive to the direct military advantage gained.

**Conclusion:** While in theory Possible may avoid Article 51 complications if sufficiently careful and skilled in executing the attack, the unpredictable reality of internet architecture, and the subsequent risk of collateral civilian damage, should raise alarm bells questioning the military value of the attack compared to the possible civilian damage. Should Possible engage in an electronic attack against Hypothetica, Possible must tread carefully in order to avoid falling afoul of Article 51.

**II (b): What if Possible attacks the physical internet infrastructure of Hypothetica existing within Hypothetica’s borders?**

Any attack on a system's physical integrity will cause the system itself to malfunction. The internet is not immune to such exposure and requires physical stability and maintenance in order to operate.

The infrastructure on which the internet operates is primarily composed of the computer hardware sending and receiving traffic, and the telecommunications cables through which data is transmitted. Any physical, brute force attack that destroyed or disconnected this physical infrastructure could, subject to the importance of the infrastructure (individually and in the aggregate), disable the internet to the extent where it was rendered effectively useless. This may be through causing data to be unavailable, or by reducing the capacity of the remaining infrastructure to carry the volume of traffic required for ordinary use.

Precision strikes on physical infrastructure have some advantage over electronic attacks: if a data centre, network hub or other physical infrastructure is known to operate solely or primarily for military purposes, a physical attack on the infrastructure carries with it less risk of causing indiscriminate damage in breach of Article 51 compared to an electronic attack.

Of course, the reality is not so simple. There are definite performance benefits in centralising internet infrastructure, and it is very likely that infrastructure is shared between military and civilian purposes. Indeed, it has been estimated that ninety-five percent of U.S. military communications are carried across public access networks at some point during transmission.[[16]](#footnote-17) During the Gulf War, seventy-five percent of communication across the war zone was carried across public telecommunications satellites.[[17]](#footnote-18) While “military-only” networks do exist, in reality the great majority of these networks are either geographically restricted (e.g. an internal network on a single military base), or exist as heavily encrypted, dedicated pathways within the publicly accessible internet.

The effect of losing physical infrastructure can be significant and is well known. For example, in 2008, workers employed by the Gold Coast City Council in Queensland, Australia, accidentally cut the main fibre optic cable for telecommunications provider SingTel Optus, causing most of the company's phone and internet network across Queensland to be entirely unusable. If a technological infrastructure attack deliberately, or even incidentally, caused the same level of service loss, it is difficult to see how the attack would not be in breach of Article 51.

**Conclusion:** If Possible attacks Hypothetica's physical internet infrastructure, and is certain that the infrastructure is solely or predominantly operated for military purposes, Possible will not be in breach of Article 51. However, it is more likely that the majority of Hypothetica's military internet infrastructure shares some connection with its civilian infrastructure, in which case the potential for civilian damage may render such an attack unjustifiable.

**II (c): What if Possible attacks the physical internet infrastructure which is outside Hypothetica but on which Hypothetica relies?**

The internet is not insular to any region, and is predominantly reliant on a network of telecommunications cables for the global transmission of data. Depending on the geographic position of the state, it may be possible to target and destroy these cables, causing international internet connectivity to be lost.

This type of attack has been known and applied for many years, and even predates the internet: undersea telecommunications cables have been the target of attack as early as World War I. Nor is the fallout of such an attack inconceivable, with a number of instances where whole regions have been disconnected from the internet at large as a result of cable breakage due to accidents or environmental events (e.g. earthquakes and tsunamis).

The consequences of such an attack will vary depending on the geographical location and development of the targeted state:

* Internet traffic in the United States is primarily internal, as most major service providers have dedicated servers within the country for providing local service. Loss of international connectivity would be bothersome but would not necessarily be significantly detrimental, at least in the short term.
* Most countries in Europe share borders, and therefore telecommunications connections, with multiple countries. Unless all these connections could be disabled by the aggressor, the targeted states' international internet connectivity may be reduced, but not completely eliminated. In practice, it is difficult to see how a single aggressor would be capable of disconnecting all such connections.
* Australia and New Zealand are developed countries with significant reliance on internet infrastructure, but due to the cost of developing infrastructure within their borders, rely on offshore providers (e.g. in Singapore or Japan) for many services. In order to access these offshore services, data must be transferred through submarine telecommunications cables lying exposed in international waters. Cutting these cables may cause significant detriment in these countries.

**Conclusion**: We do not know which of the three geographical and developmental states above Hypothetica falls into. However, it is clear that in some circumstances, a physical attack on internet infrastructure would certainly be in breach of the Article 51 prohibition against indiscriminate and excessive attack, as it is impossible to distinguish between military and civilian use of a telecommunications cable and any attack on such infrastructure would affect civilian and military purposes alike. Unless Hypothetica falls clearly into the first or second category (in which case the benefit of executing this type of attack is questionable), it may be best for Possible to avoid this method of technological infrastructure attack.

**II (d): Lessons**

From the above conclusions, I find that three common factors have been consistently implied throughout:

1. All three methods of attack run a not insignificant risk of causing damage to civilian objects or otherwise exposing civilians to danger. While in certain circumstances the attacks may be executed while avoiding these risks, the practicalities of doing so (particularly in a time of conflict), and the risk that alleviating measures may fail, may outweigh the benefit of the attack.
2. The potential fallout of all three methods of attack is contingent on the level of development of the target state. Attacks on states which are substantially reliant on internet infrastructure have a greater risk of exposing civilians or civilian objects to damage or danger than states which lack significant internet infrastructure, as demonstrated by the examples of Estonia and Georgia above.
3. The potential fallout is also dependent on how the internet infrastructure of a state is applied. For example, Estonia provides an example of how a country may become near totally reliant on the internet: both commerce and government became internet-based services, and were consequently crippled when internet capacity was lost. By comparison, a similar attack on a country like Australia or the United States may be less (but still) detrimental due to a lesser level of internet saturation and dependency.

Part of the problem in considering potential breaches of Article 51 is to what extent the internet must be crippled before the internet becomes unusable in practice. Certainly, one would be able to use a dial-up connection to access the internet today. However, it has been many years since developed countries moved to more advanced communication technologies offering greater speeds, and very few internet services remain optimised for low-bandwidth connections. Similarly, the internet is only useful due to the services available via the infrastructure: if those services are removed (whether by directly targeting the data centres from which those services operate, or otherwise disabling connectivity between the data centres and the target state), the internet may become unusable as a tool while the bulk of infrastructure remains functional.

Another problem is quantifying the damage. Dinstein suggests that only loss of life, injury, or widespread destruction of property should be taken into account when considering the danger to civilian populations. This is certainly consistent with the existing consideration of the relevant law and custom. Thus, for example, a conventional attack which resulted in many civilian casualties, or destroyed a great deal of civilian property or property essential to the survival of the population, would be prohibited, but attacks which resulted in mere inconveniences (food rationing, brownouts, shortages of non-essential goods, etc) are acceptable (where there is a greater military benefit). In the context of a technological internet attack, it is difficult to quantify what internet services are “essential to the survival of the population” versus “mere inconveniences”. Some circumstances would be clear cut (e.g. Facebook and Youtube are unlikely to be considered essential to the survival of the civilian population), and others less so (e.g. a hospital being rendered unable to access centralised medical records would certainly be an inconvenience, but is it essential to civilian survival?).

To answer this question, I return to the precise question which I sought to answer (emphasis added):

If Possible attacks Hypothetica's internet infrastructure, and Hypothetica **subsequently loses critical internet services or the internet generally is crippled to the point that the it is rendered unusable by Hypothetica's citizens,** is Possible in breach of Article 51 of Protocol I to the Geneva Conventions?

The question which I have asked explicitly focused on technological infrastructure attacks resulting in the loss of critical internet services or unusability of the internet generally. This is beyond those outcomes that are mere inconveniences, and focuses directly to those consequences which indisputably cause the civilian population substantial hardship. I am satisfied that, in the context of the question as asked, such an attack by Possible would be a breach of Article 51.

**In conclusion, I** find that a technological infrastructure attack by Possible, which causes Hypothetica to lose critical internet services or which otherwise renders Hypothetica's internet unusable, may be in breach Article 51 *where the consequence of the attack is the loss of critical internet services or the internet itself is rendered unusable*. Other circumstances where lesser damage or harm is incurred by the civilian population or civilian objects, however, remains a grey area resolvable only on the circumstances of the attack.

As a coda to the above, the interdependencies inherent in the internet may give rise to circumstances where civilians in states which are not party to the conflict also suffer some hardship beyond that which might otherwise be expected where a neighbour or trade partner is engaged in conflict. For example, Singapore is a major provider of online services in the South-East Asia region. Attacking Singapore's internet infrastructure may result in harm not only to Singapore's civilian population, but also the civilian population of any other state which relied on services operated from Singapore. These complications may result in further difficulties for an aggressor engaging in technological infrastructure attacks under international humanitarian law.

**Part III: technological infrastructure attacks and the failure of international humanitarian law**

**III (a): The threshold of suffering**

As discussed, it is not expected that civilians are immune from suffering during war. The general inconvenience of supporting a conflict will inevitably cause some hardship amongst the civilian population. Thus, there must be some spectrum of hardship which may be incurred by civilians, at some point crossing a line beyond which the hardship becomes not merely an ordinary consequence of conflict but a danger against which the civilian population should be protected.

As above, Dinstein suggests that only loss of life, injury, or widespread destruction of property should be taken into account when considering the danger to civilian populations, and this view is consistent with historical approaches to international humanitarian law. The difficulty in accepting this view is that the internet is a new creation unlike anything which has previously existed. The degree of dependency and interconnectivity of internet services, and the increasing reliance on such services, means that an attack on non-internet infrastructure that would otherwise have been considered an inconvenience causes possibly prohibitively, significant detriment when carried out against the internet analogue. For example, while physical damage to power lines may cause temporary blackouts or brownouts, a complete failure of the electricity network due to a technological infrastructure attack is a more significant loss. Other difficulties arise where we have become dependent on internet-facilitated computation to manage tasks, e.g. the logistics of food distribution is largely computerised based on production and demand, and may be rendered effectively impossible to manage were the relevant services disabled, with obvious consequences. Further, such attacks may disrupt civilian life to such an extent that the attacks become attacks causing terror in the civilian population, as prohibited by Article 51(2).

Hathaway and Crootof suggest that the injury or damage sustained by an electronic technological infrastructure attack may be “nonlethal or temporary, yet severe”, drawing a comparison between the mere inconvenience of being unable to transfer general information and the severe consequence of loss of life due to hospitals being unable to coordinate vital information (e.g. patient information).[[18]](#footnote-19) As discussed when considering the varied nature of technological infrastructure attacks, the consequences will vary dependent on the extent of adoption of internet services for the support of society by the targeted country.

This is a reasonable consideration. Undoubtedly, harm will be suffered which is short of injury, death, or massive property destruction, but nonetheless causes severe difficulties to the civilian population. However, international humanitarian law does not generally acknowledge the principle of “nonlethal or temporary, yet severe”. Even Article 51, perhaps the broadest codified general recognition of the need to protect civilians, only provides that civilians should be shielded from danger or attack, not that they are immune from suffering. This is dangerous legal territory, as even the most severe nonlethal harm may subsequently be justifiable. Certainly, a broader interpretation of “danger” and “attack” would resolve the solution, and may be appropriate with developments since international humanitarian law was last revised in this respect, but whether a tribunal would consider a broader interpretation (and whether such an interpretation would be recognised or enforced by the global community) is uncertain.

**III (b): Recognising technological infrastructure attacks under international humanitarian law**

Considering the multitude of issues surrounding technological infrastructure attacks, the obvious solution would be to explicitly recognise such attacks in codified international humanitarian law, as was done after the Second World War and the horrors of massive aerial bombing became apparent. The practicality of doing so is another question.

Many have proposed a new treaty system to recognise technological infrastructure attacks on some level.[[19]](#footnote-20) Such proposals generally include recognition of the kinds of attacks which are permitted and prohibited, and establish individual protection regimes for specific systems along the same lines as those for facilities containing dangerous forces, hospitals, cultural and religious facilities, etc. It is suggested that such a treaty would resolve the ambiguities I have discussed and provide an effective means of regulating attacks on internet infrastructure.

I must respectfully disagree with this view. I acknowledge that it may be hypothetically possible to establish a treaty system, or amend existing treaties, to acknowledge *jus ad bellum* questions regarding electronic technological infrastructure attacks (i.e. cyber attacks) and the rights and obligations of signatories in the exercise or prevention of such attacks. However, I believe that the difficulties in drafting such a treaty, particularly regarding the status of the internet as a hybrid civilian and military object and the protection of civilians as I have discussed in this paper, is doomed to fail.

On a practical level, an obvious problem arises in simply defining a technological infrastructure attack. I have proposed one definition, being “any action by a state, by physical or electronic means or otherwise, to undermine the functions of the internet of another state.” While this has been adequate for my discussion, I hold no illusions that such a general definition would be accepted by the global community, which would inevitably demand a more precise definition with the equally inevitable subsequent “black-letter law” interpretation by states engaging in such conduct. While this may resolve the greyness of the area, it would also result in many attacks which should reasonably be considered crimes being excluded, potentially leaving the determination for such conduct to the idiosyncrasies of a future kangaroo war crimes tribunal.

The rapid development of technology also makes it difficult to create a specific definition of a technological infrastructure attack, or laws regarding technological infrastructure attacks, in a way which will stand the test of time. Codified international humanitarian law is sporadically updated and it is likely that any specific definition would soon be out of date. The time it would take the international humanitarian law to come to agreement on such a definition or law would not assist. Per Walker, “any international agreements... would likely be obsolete in terms of hardware and practice before their ink would be dry.” I am inclined to agree.

Finally, judging the detriment that may be incurred by a civilian population is not something that is likely to be determined simply by reference to some abstract quantitative set of rules: it is always going to be an emotive and qualitative process. Nor should it be: as discussed, the multitude of means by which internet infrastructure may be disabled, and the multitude of ways in which civilians may suffer as a result of such an attack based on the extent of their country's reliance on the internet and their geographical location, eludes easy definition.

The simple reality is that any technological infrastructure attack is, with few exceptions, fraught with uncertainty. The constantly changing and evolving nature of the beast which is the internet and its increasing pervasiveness in global society is something which cannot be encapsulated in a treaty expected to stand for a fraction of the time that existing treaties have been in force. While realistic, I am conscious that this is an unsatisfying answer.

**III(c): The success of international humanitarian law**

And yet, it is not necessarily a complete failing of international humanitarian law. At the time of the bombing of Dresden, aerial bombing had not been explicitly considered in the laws of war. The fact that the legality of Dresden has been debated for 67 years (as of this writing) indicates that, as then, it may not be necessary to recognise the specific technologies used. In what has been a recurring theme throughout this paper: the means of the attack are inconsequential with respect to the consequences. While the letter of the law may not be settled to an extent where it may be reliably enforced by a war crimes or human rights tribunal, there is something of a question as to whether enforceability is necessary in order for the benefit to exist.

It has never, in reality, been the situation that codified international humanitarian law was an international analogue to a state's criminal code or similar legislative instrument. The practical difficulties in enforcement, at this time, preclude any such adoption of the law. Rather, international humanitarian law has stood in practice to regulate the conduct of states before, during and after conflict as such conduct occurred, i.e. it serves to prevent such attacks, rather than provide justice after their exercise (this being the purpose where the preventative expectation has failed).

Hathaway and Crootof suggest that cyber attacks may change the way in which states consider technological infrastructure attacks and international humanitarian law. The difficulties in mounting a technological infrastructure attack while avoiding any breach of international humanitarian law are not insurmountable, but extra care must, and likely will, be taken by any state considering a technological infrastructure attack. As has been said by so many, “war is hell”, and it is unlikely that any country sufficiently advanced to mount an effective technological infrastructure attacks would also be willing to risk setting the precedent that, at least in the context of technical infrastructure attacks, civilians are “fair game” so long as they are not directly harmed and will choose to withhold attacks with potentially excessive consequences for the sake of caution. With increasing reliance on the internet globally, it will be far more difficult to approach any technological infrastructure attack otherwise with respect to the potential civilian consequences. In this respect, and not in an enforceability respect, does the strength of current international humanitarian law lie.

**Conclusion**

**If Possible attacks Hypothetica's internet infrastructure, and Hypothetica subsequently loses critical internet services or the internet generally is crippled to the point that the it is rendered unusable by Hypothetica's citizens, is Possible in breach of Article 51 of Protocol I to the Geneva Conventions?**

In considering this question, it has been necessary to consider the multitude of ways in which my imaginary state Hypothetica's internet may be attacked, these being electronically, physically within its borders, and physically outside its borders, with such attacks occurring singularly or in combination. Each has its own benefits and drawbacks with respect to the ability of Possible to target military objects and avoid civilian objects, but ultimately all methods of attack carry some inescapable risk that some peripheral damage to civilian objects will occur.

From this, in the context of Article 51 (being the broadest article of international humanitarian law with respect to the protection of civilians and civilian objects), the two issues that arose were the indiscriminate nature of technological infrastructure attacks, and the internet itself as both a legitimate military object with definite military value as a target and as a civilian object which, if damaged or disabled, may cause significant hardship to Hypothetica's population.

Possible is not prohibited *per se* from attacking Hypothetica's internet infrastructure. An attack by Possible on a legitimate military target is by no means a breach of any international humanitarian law, even if it is an internet-based object, and conversely a deliberate attack on civilian internet will certainly result in Possible breaching the law. However, any technological infrastructure attack is, due to the nature of the internet, an inherently indiscriminate attack, and great care will be required on the part of Possible in order to avoid drawing civilians into the line of fire. Careless exercise of a technological infrastructure attack may, in the circumstances, result in Possible cyber-bombing Dresden, in breach of Article 51 and, in all probability, other articles of international humanitarian law.

As to the internet as both a military and civilian object, it is clear that the question remains in the air. The internet is not an inherently protected object. However, the issue of proportionality is a significant one. The only final conclusion that may be drawn is that the greater the suffering inflicted on the civilian population, the closer Possible will come to affecting civilians to an extent greater than the military advantage offered by the technological infrastructure attack. If Possible is to avoid breaching Article 51, it may be best simply to not utilise technological infrastructure attacks at al.

On a more general level, there are many issues facing states with respect to technological infrastructure attacks and civilians under international humanitarian law. In many respects, international humanitarian law is not adequate for the technology of today, and I do not expect that it ever will be due to the rapid march of progress.

However, it may be that this question may resolve itself simply through the passage of time and further adoption of the internet as a social tool. As Hypothetica (and the world generally) develops new services and methods for leveraging the internet for the benefit of the ordinary life of its citizens, Hypothetica will suffer correspondingly greater detriment should its internet be crippled (by any means) by Possible to the point it becomes unusable. At some point, a saturation point will be reached where, while theoretically possible, the practical effect of such a technological infrastructure attack will endanger or terrify the civilian population to such an extent that a technological infrastructure attack not carefully and specifically targeted solely to a legitimate military target becomes untenable. In this, international humanitarian law may yet succeed.

1. http://www.dresden.de/media/pdf/infoblaetter/Historikerkommission\_Dresden1945\_Abschlussbericht\_V1\_14a.pdf [↑](#footnote-ref-2)
2. LT Greenberg et al, Information Warfare and International Law at 10-11 [↑](#footnote-ref-3)
3. Article 54 P1 GC4 [↑](#footnote-ref-4)
4. Article 54 P1 GC4 [↑](#footnote-ref-5)
5. Article 53 P1 GC4 [↑](#footnote-ref-6)
6. Article 51 P1 GC4 [↑](#footnote-ref-7)
7. ~1900's international law treaties e.g. Hague 4 [↑](#footnote-ref-8)
8. LT Greenberg et al, Information Warfare and International Law at 12 [↑](#footnote-ref-9)
9. JA Lewis, A Note on the Laws of War in Cyberspace, CSIS [↑](#footnote-ref-10)
10. [↑](#footnote-ref-11)
11. S J Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law [↑](#footnote-ref-12)
12. SW Korns & JE Kastenberg, Georgia's Cyber Left Hook [↑](#footnote-ref-13)
13. At 826 [↑](#footnote-ref-14)
14. JTG Kesley, Hacking into International Humanitarian Law: the Principles of Distinction and Neutrality in the Age of Cyber Warfare at 1437-8 [↑](#footnote-ref-15)
15. Hathaway and Crootof at 852. [↑](#footnote-ref-16)
16. [↑](#footnote-ref-17)
17. [↑](#footnote-ref-18)
18. At 851 [↑](#footnote-ref-19)
19. Rowe at 4 [↑](#footnote-ref-20)