The Implications of New Technology for Copyright Law and Intellectual Property

Copyright law and intellectual property rights have been a longstanding concern of the international community. The Universal Declaration of Human Rights and the International Covenant on Economic, Social, and Cultural Rights both recognize intellectual property as a human right.¹ The United Nations Educational, Scientific, and Cultural Organization (UNESCO), as well as other international bodies, have made various recommendations to help protect the rights of copyright holders. Actions taken to protect copyright and intellectual property have been threatened by the emergence of new technologies that make it easier for people to illegally access protected works. Despite the global nature of this problem, there is no universally accepted solution, and most laws and regulations exist at the national level. UNESCO member states should examine how the international community can improve upon existing treaties and how they can be adapted to fit the demands of the rapidly evolving digital environment.

One of the most pivotal steps towards a global approach to copyright laws and intellectual property was the formation of the World Intellectual Property Organization (WIPO) in 1967.² Its purpose, as stated by Article 3 of the Convention to Establish the World Intellectual Property Organization, is “to promote the protection of intellectual property throughout the world through cooperation among States and, where appropriate, in collaboration with any other

international organization.” WIPO defines copyright as the legal rights that creators have over their literary and artistic works and intellectual property as the rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields.

Since the creation of WIPO, innovations in digital technologies and their increasing availability have challenged the traditional balance between access to copyrighted materials and the rights of their producers. With the invention of technologies including the internet, file-sharing services, and, most recently, 3-D printing, individuals are able to access, reproduce, and distribute copyrighted materials more widely and often at no cost. In many countries, piracy and counterfeiting have become low risk and high profit crimes, with few legal repercussions to deter infringers. UNESCO has noted the negative impacts on cultural industries and development, which can’t compete with low cost of pirated or counterfeit goods. Piracy and counterfeit trade has also been linked to organized crime, its profits used to fund other crimes, such as human and gun smuggling, drug trafficking, and money laundering. Regardless of these challenges, the economic value of copyright industries globally has reached an all-time high, accounting for billions of dollars and millions of jobs.

Consisting of 185 member states, WIPO has been instrumental in coordinating a global approach to these issues. As a special agency of the United Nations, WIPO offers a range of global services for protecting intellectual property across borders. Three of its most important services are the International Patent System, the International Trademark System, and the

International Design System.\(^7\) Administered by WIPO and established by the Madrid, Hague, and Lisbon treaties respectively, these services allow businesses and individuals to register patents, trademarks, and designs in multiple countries at once.\(^8\) Businesses can also use arbitration and mediation resources offered by WIPO to settle intellectual property battles outside of court and across borders.\(^9\) In order to help facilitate the use of these services in developing countries, WIPO also offers technical training and capacity building tools to regional and national organizations. These services include online registry and filing systems, access to electronic databases, and educational materials on copyright and intellectual property law.\(^10\)

Many of the WIPO administered treaties have played a key role in shaping the international approach to copyright law. One of the earliest intellectual property treaties, the Berne Convention for the Protection of Literary and Artistic Works of 1886 is now overseen and revised by WIPO. Last amended in 1979, the Berne Convention provides the basis for many of the treaties and agreements that have since followed.\(^11\) Protections outlined by the convention include automatic copyright, meaning signatories are prohibited from requiring formal registration of works, and the length of copyright terms.

In 1996, the international community adopted two WIPO administered treaties to address the growing concern over digital copyright and intellectual property, the first of which is the WIPO Copyright Treaty (WCT). The WCT addresses the protection of works and rights of their creators in the digital environment.\(^12\) It grants authors the right of distribution, the right of rental,

\(^8\) Ibid.
\(^9\) Ibid.
\(^10\) “Cooperation,” World Intellectual Property Organization, [www.wipo.int/cooperation](http://www.wipo.int/cooperation)
and the right of communication to the public to the authors of protected works. In addition to the protection of traditional media, the WCT also acknowledged the protection of computer programs and some databases.\textsuperscript{13} The second is the WIPO Performances and Phonograms Treaty, which grants audio performers the economic rights in the performances on fixed phonograms, as well as the right to distributions, the right of rental, and the right of making works available.\textsuperscript{14} It also grants them rights to object to any modification of their work and certain rights to live performances.\textsuperscript{15}

Known collectively as the Internet Treaties, these agreements have hugely influential in the discussion of technology and intellectual property. The Internet Treaties have influenced legislation on the regional and national level. One notable example is the Digital Millennium Copyright Act of 1998 in the United States, which criminalizes the use of technology and services that violate copyright law.\textsuperscript{16} Similarly, the European Union Copyright Directive was adopted in 2001, which added several provisions to the Internet Treaties, including the right of reproduction in the digital environment, and the technological measures for protection.\textsuperscript{17}

In addition to WIPO, the World Trade Organization and UNESCO have also administered intellectual property-related agreements. One of the most significant of these agreements is the WTO Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS). Adopted in 1996, TRIPS seeks to set minimum standards for copyright protection

\footnotesize
\textsuperscript{13} Ibid.
\textsuperscript{15} Ibid.
\textsuperscript{17} Ibid.
amongst WTO members while respecting their diverse legal systems. It also established the TRIPS council, which examines how states apply the principles of the agreement. TRIPS is one of the most widely recognized intellectual property treaties, as all 158 members of the WTO are party to the TRIPS Agreement. UNESCO intellectual property agreements have largely been focused on the protection of cultural artifacts and traditions. To this end, UNESCO has administered a number of agreements to safeguard cultural property, including the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, the Convention for the Safeguarding of the Intangible Cultural Heritage, and Convention on the Protection and Promotion of the Diversity of Cultural Expressions.

Despite efforts toward international cooperation, copyright law has been a source of tension between several countries. China, a member of WIPO since 1980, is often cited for the high level of copyright violations within the country. In 2007, the International Federation of the Phonographic Industry estimated that almost 99% of all music accessed online in China violated copyright laws. The Chinese government has come under fire for policies that fail to enforce copyright laws. In 2007, the United States filed a formal complaint with the World Trade Organization over China’s refusal to grant copyright protection to works that had not been approved by government censors. In 2009, the WTO ruled that China had violated existing trade agreements. The various actions taken by multinational organizations and regional

---

19 Ibid.
23 Ibid
governments have done little to halt the spread of copyright piracy online. Researchers estimate that between 400,000 and 600,000 films are downloaded through file sharing networks and unauthorized video streaming websites daily.\textsuperscript{24} In addition to the illicit distribution of films, copyright holders have to contend with the growing popularity of fan films featuring characters used without permission. WIPO has proposed the creation of a treaty to address the concerns of broadcasting organizations and provide internet-specific protections that might not be covered by other agreements, such as TRIPS.\textsuperscript{25} Another increasingly popular technology that has copyright holders concerned is 3-D printing. 3-D printing, also called direct digital manufacturing, allows users to create objects from digital files. While not nearly as accessible as other innovations mentioned, experts have already hailed 3-D printing as the “democratization of manufacturing.”\textsuperscript{26} There is growing concern that 3-D printing will make it easier for people to share and copy object designs, and that the ease of producing these copies will lead to decreased investing on research and development by manufacturers.\textsuperscript{27} Intellectual property policymakers have struggled to find a way to protect these designs while encouraging exploration of the technology and further innovation.

The push for greater control of intellectual property by the major copyright industries has been the center of growing controversy over the past decade. The widespread use of the internet has often been touted as a way of removing barriers to accessing knowledge, sometimes at the expense of copyright holders. Opponents of expanded digital copyright laws argue that these protections reduce the ability of individuals and states to ensure that copyright meets its basic

\textsuperscript{25} Ibid
\textsuperscript{27} Ibid
goals of expanding the pool of available knowledge. In 2012, the Human Rights Council adopted A/HRC/20/L.13, which asserted that the same rights that people have offline are also protected online, and encouraged states to promote and facilitate access to the internet. There is growing concern that efforts to establish global copyright laws will impede the flow of information, especially in regards to developing countries. Recent efforts to establish international agreements on intellectual property rights have been met with great resistance. In 2011, Australia, Canada, the European Union, Japan, Mexico, Morocco, New Zealand, Singapore, South Korea, Switzerland, and the United States began negotiating the conditions of the Anti-Counterfeit Trade Negotiation. The treaty, which exists outside of any existing international organizations, establishes international guidelines for the enforcement of intellectual property laws. Shortly after the agreement’s formal publication, thousands of Europeans took to the streets in protest. Protesters argued that ACTA would stifle freedom of expression over the internet and the lack of transparency in its negotiations. Government support for ACTA quickly declined. While many of its negotiators are now signatories, only one country (Japan) has ratified the treaty.

Addressing copyright law and intellectual property rights on the international level is a complex issue, made more difficult with today’s rapid technological advancements. So far,

---

31 “Anti-Counterfeiting Trade Agreement” Office of the United States Trade Representative (2012), http://www.ustr.gov/acta
33 Ibid.
efforts toward a global approach have been wrought with controversy and debate. UNESCO members must address how to settle copyright disputes between countries with vastly different copyright laws, while maintaining national sovereignty. Members of UNESCO must examine how the international community can protect intellectual property rights while respecting national laws, the freedom of expression, and the right to access information.

Questions:

1. What laws and regulations regarding copyright and intellectual property does your state have in place? What can the international community take away from the successes and challenges of these laws?

2. In what ways can the current UNESCO and WIPO treaties and agreements on copyright law and intellectual property be improved?

3. What is the relationship between intellectual property, copyright, and access to knowledge? How does the right to internet play a role in this debate?

4. While there has been a growing push for digital copyright regulations, it is often remarked that laws have been slow to catch up to technology. How can the international community ensure that its efforts are consistently up-to-date with current technology?

5. Some human rights activists claim that expanded enforcement of digital copyright law could encroach upon free speech. How can countries deter online piracy without infringing upon the right to expression over the internet?

6. What are the implications of international standards for intellectual property rights?

**Bibliography**


“What is copyright?” *World Intellectual Property Organization.*


Although it is generally understood what constitutes a cyberattack and what does not, there is no internationally agreed upon definition of a cyberattack. Since there is no consistency, as technology and society advances it makes it increasingly difficult to combat such attacks. The tactics of cyberterrorists are constantly evolving, such as in the case with the Stuxnet virus in Iran, and yet the world remains undecided on a comprehensive definition to address the evolving cyberworld.

Cyberwarfare: What is it?

One of the largest difficulties with applying international law to cyber attacks is the lack of consistency in the definitions that constitute these attacks. The literature on “cyber attack(s)” reveals two predominant understandings of the term: some speak of the use of computers and computer networks as *instruments* of attack, and some speak of computers and networks as the *objects* of attack.”¹ However, both of these definitions still leave out integral parts of what constitutes cyberwarfare. The U.S. National Research Council defined cyber attack as “the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident

---

in or transiting these systems or networks.”\(^2\) This definition, although broad and encompassing, still makes no mention of the means by which the attacks have been conducted. By focusing on the objects of the attacks, it seems as though conventional weapons such as bombs and missiles could “…alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks,” much the same that “electromagnetic pulse energy can be manipulated to overwhelm computer circuitry or jam communications.”\(^3\) Since definitions focusing on the objects of attack are overly broad and therefore malleable, it makes sense to focus on the definition of a cyber attack as one that describes the \textit{means} of the attack. For example, an “air attack” is commonly understood to be an attack \textit{from} the air and not \textit{on} the air, much in the same way a “cyber attack” ought to refer to an attack through cyberspace and not necessarily on it. Since there is no internationally agreed upon definition of a cyberattack, the most scholarly and all encompassing definition of cyberwarfare is, according to the California Law Review:

\begin{quote}
 a hostile act using computer or related networks or systems to cause disruption or destruction for a political or national security objective. Under this construction, a cyber attack is hostile (as such is the nature of attack) and uses computers or their networks to conduct the attack, but leaves open what type of disruption or damage it may cause. The attack is constrained only by its political or national security objective, which distinguishes a cyber attack subject to international law from a cyber crime subject to domestic law. \(^4\)
\end{quote}

The anatomy of a cyber attack has two main components: exploiting the target’s weaknesses and delivery of the payload. The weaknesses constitute susceptibility or a flaw in the


\(^3\) Navigating Jus Ad Bellum, 1087

\(^4\) Navigating Jus Ad Bellum, 1089-1090
system, an access path for reaching that flaw, and the hacker’s ability to exploit the flaw. The payload that is delivered by the hacker refers to the actions (depending on the motive of the attack) that can be executed once the flaw has been exploited. Almost every cyber system has inherent characteristics and/or flaws that can leave it vulnerable to an attack. Such vulnerabilities can include “…design or implementation defects introduced inadvertently or intentionally into software, hardware, or the seams between software and hardware.” It is also possible for an attacker to hide as an authorized user to attack communication channels, other legitimate users, or service providers. A cyberattack can gain access “…remotely through networks, or locally through close access, such as insertion of data-carrying external media (such as USB thumb drives), local software or hardware installation (compromised third-party security software), or elsewhere in the system supply chain (during design, development, testing, production, distribution, or maintenance).”

Types of Cyberattacks

There are two different types of cyberattacks that are used: Penetration Attacks and Denial of Service attacks. Penetration attacks constitute an attacker accessing a system either directly or remotely to deliver their payload, thus allowing them to “access or alter files for a variety of objectives.” One of the most common objectives of a penetration attack is to deliver Malware. Malware “is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other ‘bad’ or illegitimate action on data, hosts, or networks.” Malware is especially dangerous because the code will be written to automatically execute the payload and

5 Navigating Jus Ad Bellum, 1092
6 Ibid
7 Navigating Jus Ad Bellum, 1094
self-propagate, thus making it more dangerous than an attacker’s direct manipulation.\footnote{Navigating Jus Ad Bellum, 1094} Some of the most common forms of Malware are viruses, worms, Trojans, and bots.

Viruses will attach themselves to software inside of the victim’s computer, “using that software to execute its payload to alter or damage the computer, self-replicate, and spread to other computers when the host file or program to which the virus is attached is intentionally transferred from one computer to another.”\footnote{Navigating Jus Ad Bellum, 1094-1095} Viruses are very similar to Trojans, the only difference being the manner in which the Malware is spread. Trojans will disguise themselves as trusted and legitimate forms of software that once opened by the unsuspecting user will infect their computer. Trojans, however, “do not self-replicate, unlike true viruses and worms.”\footnote{Navigating Jus Ad Bellum, 1095} Worms are very similar to viruses, in that they self replicate; however, viruses require the sharing of an infected file, but worms will replicate independently of the infected files. In order for worms to spread, they seek out a vulnerability in one computer and network and use the existing file-transport or information transport features contained within the system, thus allowing them to travel unaided. Due to this feature of self-propagating, worms will spread at a much faster rate than viruses. Finally, and quite possibly the most dangerous of the types of Malware, are botnets. Botnets are an assortment of hundreds to hundreds of thousands (and possibly even a million) different infected computers with viruses, Trojans, and/or worms that allow a single attacker, or “botmaster,” to hide behind a virtual army of “zombie-bots”, which can then be controlled remotely by the botmaster. “A continuous broadband connection facilitates a communications channel between the botmaster and his zombie-bots, which may initially sense and probe their immediate environment, examine system files, and relay the
information to the botmaster. With the benefit of this information, the botmaster can then upgrade that merely investigatory payload to a destructive payload specifically tailored to the target system.”

The most dangerous aspect of the botnets is the relative anonymity they provide to the botmaster, and, obviously, the destructive capabilities of a botnet. “The zombie-bots…serve as further attack intermediaries that provide a buffer between the botmaster and his targets and conceal the source of attack.”

Aside from penetration attacks there are also Denial of Service (DoS) attacks. These attacks are not as malicious in nature as penetration attacks because they do not delete or alter computer system resources, but their effects can cause very real issues by:

flooding a specific target with bogus requests for service, thereby exhausting the resources available to the target to handle legitimate requests for service and thus blocking others from using those resources. Since attacks coming from a single source can easily be blocked by denying all requests from that source, attackers employ botnets to conduct distributed denial-of-service (DDoS) attacks from multiple machines.

Because there are requests from thousands to hundreds of thousands of users, the server is unable to differentiate between real users and attack zombie-bots, therefore the attack becomes almost impossible to stop since the attack cannot be stopped from a single source. Although DDoS attacks seem to be nothing more than a mere nuisance, they can still cripple the systems they are attacking. For example, in the 2007 Estonian DDoS attack there were in upwards of one million zombie bots used as a part of an organized botnet, each in control of thousands of computers. These zombie bots mercilessly flooded government, media, and financial institution websites,

---

12 Navigating Jus Ad Bellum, 1095-1096
13 Navigating Jus Ad Bellum, 1096
14 Navigating Jus Ad Bellum, 1097
thus rendering these sites inaccessible for hours at a time. This attack was especially crippling for Estonia due to their heavy use of information technology.\textsuperscript{15} As the world becomes more and more dependent on information technology, the very real consequences of DDoS attacks will be larger and larger as well.

**Major Issues in Combating Cyber Attacks**

As technologies advance, so do the methods by which various actors perform illegal activities. In today’s society, many different physical systems are controlled by computers and microprocessors, thus making the threat of cyber attacks much more difficult and complex. Traditionally, cyberattacks and Malware have only had direct effects on the systems that they attacked, but now with the rise of cyber-physical technology those effects have much more damaging and unintended consequences. For example:

In 2010, the Stuxnet worm, a self-replicating computer virus targeting computers that regulate automated physical processes, took control of Iran’s nuclear centrifuges at Natanz and caused about one-fifth of them to spin out of control and self-destruct. Iran’s uranium enrichment operations halted, resulting in an estimated several years of delay in the country’s nuclear arms development program. Responsibility for Stuxnet has been attributed to Israel and the United States.\textsuperscript{16}

Because this attack was on the computers controlling the centrifuges and not the centrifuges themselves, this would put any indirect attack on cyberphysical systems in a legal gray area, due to the indirect nature of the attack.

Further, the unintended consequences of cyberattacks also complicate the issue given that other systems can be harmed or disabled by various sorts of cyberattacks:

\textsuperscript{15} Navigating Jus Ad Bellum, 1097-1098
\textsuperscript{16} Navigating Jus Ad Bellum, 1082
the Sapphire worm took down servers in South Korea, the suspected target of the attack, but its consequences were more wide-ranging. Sapphire also disrupted internet services in Thailand, Japan, Malaysia, the Philippines, and India; disconnected a city’s 911 emergency service and caused problems for thirteen thousand Bank of America ATMs in the United States; postponed a Canadian national election; and cancelled airline flights. Moreover, because Malware is autonomous from its author and acts automatically, “...the attacker cannot scale back or halt the extent of damage once the malware is released—the damage spreads as surely as the virus or worm spreads—and an attack on systems in South Korea becomes an attack on systems in Thailand and Japan, Canada and the United States.”

Further complicating the issue in combating cyberwarfare is the inherent inaccuracies and lack of test runs with the Malware. “The malware’s targeted environment often is not and cannot be accurately reproduced before the malware is released. And in contrast to...[conventional] attacks, cyber attacks require intelligence information that is difficult to obtain through traditional intelligence methods...” The unpredictable nature of Malware makes the odds of having unintended consequences much higher.

The other glaring issue in the fight against cyberwarfare is anonymity. As discussed with the botnets earlier, attackers are able to masquerade behind a virtual wall of zombie-bots, while still having the capability to deliver a malicious payload. “Botmasters create command-and control centers that direct the bot army. These centers act as barriers that shield the originator of the attack from detection, while the innocent computer systems drafted into the botnet serve at

17 Navigating Jus Ad Bellum, 1100
18 Navigating Jus Ad Bellum, 1101
19 Navigating Jus Ad Bellum, 1102
the front lines of attack.” Further complicating this issue is that the main source of identifying people’s exact location via the Internet—IP Addresses—is easily circumvented. “…Because these…[IP addresses] are often transmitted without mechanisms to authenticate their origin, the source IP address can easily be forged, or “spoofed,” to conceal the sender’s identity. Thus, this ability to easily conceal one’s identify by “spoofing” their IP address allows the attackers to remain virtually anonymous.

Problems with International Law Governing Cyberwarfare

Cyberattacks have emerged only in recent times as technology has advanced, which makes it very hard for them to be governed by international law due to the lack of precedent and clear definitions in the U.N. Charter or treaties and conventions. Due to this lack of precedent in international law, “fundamental differences among the world’s major cyber-powers about the scope of activities that should be prohibited under an international cyber attack agreement.”

The most common passage in the Charter that is cited to defend the United Nation’s right to govern cyberwarfare is in Chapter 1, Article 2, subsection 4 of the U.N. Charter, which states “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” Further, Article 51 of the charter proscribes “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations...” Both of these definitions are equally mum about cyberwarfare. Moreover, both definitions are equally ambiguous, such that “use of force” and “armed attack” are not clearly defined. At either end of the spectrum it is easy

20 Navigating Jus Ad Bellum, 1105
21 Navigating Jus Ad Bellum, 1111
22 Charter of the United Nations
23 Ibid.
to tell what *is* and what *is not* a use of force, but what exactly constitutes an “armed attack” and thus retaliatory measures by the victim state has been debated for decades. In Nicaragua v. United States, the case most important case that interpreted Articles 2(4) and 51 of the U.N. Charter, the International Court of Justice (ICJ) found that not every use of force constituted a retaliatory attack. Despite this finding, the ICJ declined to define “use of force” or “armed attack” “or to address what would constitute permissible responsive action, if any, when force falls short of armed attack.” Since the Charter is so ambiguous and the ICJ has declined to clearly define these terms, the only option is to look to cases such as Nicaragua v. United States to show examples of what is and what is not an armed attack.

While the exact definition of an armed attack, or the definition of a cyberattack in general, is not yet settled in the international arena, the international community has addressed the defensive side of the issue in numerous ways. The General Assembly adopted Resolution 58/199 in 2004, establishing guidelines for protecting what are termed “critical information infrastructures,” including power, transportation, finance, food, water and health infrastructure. Similarly, according to the report “Cyberwarfare and International Law,” published by the United Nations Institute for Disarmament Research, while a cyberattack is difficult to define, any variety of cyberattack that rises to the level of a use of force constitutes an armed conflict to which international humanitarian law applies. As such, the development of guidelines for defining cyberattacks - and defining the level at which a cyberattack becomes a use of force - is absolutely vital to not only defending against such attacks, but also applying humanitarian protections to civilians affected by cyberattacks.

---

24 Navigating Jus Ad Bellum, 1115
One of the core ideologies of the United Nations as stated in the Preamble to the Charter is to regulate nation-states’ interactions with each other in order to avoid a third world war, but also to protect and promote human rights and human development. It makes sense then that under the U.N. Charter, the U.N. ought to act accordingly to attempt to regulate cyberwarfare. With the rise of cyberphysical technologies and the abilities to destroy them from behind a computer screen, it becomes increasingly important for the U.N. to regulate cyberattacks in the interest of preserving human rights and development. Moreover, as seen in Estonia, it is possible to render government websites and services virtually useless with DDoS attacks, thus further jeopardizing citizens’ rights and development. Cyberwarfare, in its very meaning, intends to disrupt the political independence of the victim state, thus necessitating the United Nations to take action to combat the 21st century’s new style of warfare. It is then the job of this committee to create a comprehensive definition of a cyberattack, and to create meaningful, fresh ideas in how to best regulate and govern cyberattacks.

Questions for Consideration:

1. Does your country already have a definition of what constitutes a cyberattack?
2. Does your country have the capability to either suppress or end a cyberattack?
3. What are your country’s laws currently regarding cyberattacks?
4. What is your country’s ability to withstand a cyberattack? Have they ever had to withstand a cyberattack?
5. What is your country willing and able to do to help the international community and most importantly under-developed states with regards to cyberattacks?

Bibliography


\url{http://scholarship.law.berkeley.edu/californialawreview/vol101/iss4/4}


\url{http://sites.nationalacademies.org/CSTB/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf}


https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf


\url{http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html}
Maintaining and preserving cultural artifacts and landmarks

Harnessing the power of culture and its influence on the socialization between nations continues to be one of the major tenets of the United Nations’ international policymaking efforts. Culture and heritage have been and continue to be two powerful driving forces in political and social cooperation, constituting a source of identity and cohesion for communities disrupted by bewildering change and economic instability. The United Nations Economic, Scientific and Cultural Organization (UNESCO) acts as the prime source of international policies addressing culture’s influence on contemporary global issues and affirms that a human-centered approach to social, economic and political development is essential for powerful and lasting change within the global community. As an advocate for the protection of global cultures, UNESCO has played a significant role in preventing damage to particular areas of the world known for their cultural or historic significance. UNESCO has outlined the heavy of role culture and the importance of preserving the diversity of the global community in the Universal Declaration on Cultural Diversity. Culture strengthens capacities worldwide for creation, builds partnerships in the public sector, private sector, and civil society, and draws together the common heritage of humanity. The defence of cultural diversity is an ethical imperative, inseparable from respect for human dignity. It implies a commitment to
human rights and fundamental freedoms, in particular the rights of persons belonging to minorities and those of indigenous persons. Through the protection of cultural landmarks and artifacts, as well as world heritage sites, the global community draws together under a common cause of protecting humanity’s roots, preserving precious treasures of our past and paves the way for greater global cooperation among diverse cultural groups.

One of the first examples of UNESCO taking an active role in preserving cultural landmarks was the decision to build the Aswan Dam in Egypt, which would have flooded the valley containing the Abu Simbel temples, a treasure of ancient Egyptian civilization. In 1959, after an appeal from the Egyptian and Sudanese governments, UNESCO launched an international safeguarding campaign. Archaeological research in the areas to be flooded was accelerated. The Abu Simbel and Philae temples were dismantled and reassembled with extreme precision by domestic and international efforts spearheaded by a number of Swedish firms.¹

The campaign took five years and cost about US$42 million, half of which was donated by some 50 countries, showing the importance of solidarity and nations' shared responsibility in conserving outstanding cultural sites.² Its success led to other safeguarding campaigns, such as saving the ruins at Moenjodaro in Pakistan, and restoring the Borobudur Temple Compounds in Indonesia.³ ⁴ All of these heritage sites had been damaged by natural means and faced greater threats to the sustainability to their structures. The ruins at Moenjodaro faced salinity in the groundwater, and the Borobudur

---

² Ibid.
Temple Compounds suffered from excessive tourism, stone erosion and damaged structural integrity. Consequently, with the help of the International Council on Monuments and Sites (ICOMOS), UNESCO initiated the preparation of a draft convention on the protection of cultural heritage.

In 1972, UNESCO hosted the World Heritage Convention (WHC) with the primary goal of identifying potential sites that hold essential cultural significance for global citizens as well as specific peoples within the selected site’s region. The WHC places the duties of identifying, protecting and preserving potential sites on member states. Each state party to the Convention pledges to conserve both world heritage and national heritage in the states’ territory to keep heritage sites safe in times of conflict as well as pledging to sustain the landmarks and cultural connections that helped identify the significance of the site. States are encouraged to implement regional policies and programmes to protect and preserve these sites, as well as conduct research to provide a practical purpose for the site in the everyday lives of peoples within the region. The Convention also establishes an Intergovernmental Committee for the Protection of the Cultural and Natural Heritage of Outstanding Universal Value formally known as the World Heritage Committee. Comprised of 191 member states, the committee is mandated with addressing issues regarding current World Heritage sites as well as the declaration of new sites. The WHC - both the Convention itself, and the Committee - is therefore the primary instrument for the protection and preservation of cultural landmarks and other sites of historical and cultural importance.

---

The WHC also outlines the World Heritage Fund and the commitments each state agrees to upon signing the Convention. Periodic reporting on preservation progress within each territory is crucial to the work of the Convention as they allow members to assess the conditions of each site, decide on specific programme requirements, and resolve recurring issues and conflicts.\(^7\) It also encourages state parties to strengthen the public’s appreciation for World Heritage properties and to enhance their protection through educational and information programmes. In addition to these measures, the international community had adopted numerous other instruments. In 2005, member states of UNESCO adopted the Convention on the Protection and Promotion of the Diversity of Cultural Expressions, which deliniates general guidelines for the protection of cultural expression in all its forms, both with respect to current expression and historical artifacts.\(^8\)

As of the 38\(^{th}\) session of the World Heritage Committee in 2014, there are 1007 registered World Heritage sites. Among these, 779 are labeled cultural sites, 27 of which have been labeled “in danger” by the Committee.\(^9\) In order to preserve all sites, with specific emphasis on sites endangered by forces such as natural disasters, human conflict, looting or other harmful influences, UNESCO and various governing bodies within respective regions have implemented protective policies and programmes. Some have found success in the past, while others has fallen notably short of their intended goals.

There are five regions under the World Heritage Convention: Africa, Asia and the Pacific, Arab States, Europe and North America, and Latin America and the Caribbean.

Each region sets unique objectives and has their own methods for reporting to the World Heritage Convention. For example, the Africa Region has constructed a 2012-2017 Action Plan with objectives that include but are not limited to: (1) improving the representation of African heritage sites on the World Heritage List through the preparation of successful nomination dossiers, (2) improving the state of conservation at World Heritage properties, by effective risk management, increased community involvement and direct economic benefits to local communities, and (3) effectively managing existing properties by recognising, documenting and formalising traditional management systems and fully incorporating them into existing management mechanisms\textsuperscript{10}.

Contrarily, the Asia and Pacific region, as well as the Europe and North America regions, conduct two cycles of periodic reporting in order to consolidate unique objectives and plans for the various sites in the region. The first cycle for Asia and the Pacific began in 2003, which led to the successful production of a comprehensive publication entitled “Synthesis Regional Periodic Report for the Asia-Pacific Region 2003.” The subsequent progress and follow up to the first cycle was fruitfully achieved through the implementation of two regional programmes; “Action Asia 2003-2009” and “World Heritage-Pacific 2009”, which directly respond to the conclusions, recommendations, and action plans resulting from the first cycle. The World Heritage Committee launched the second cycle of Periodic Reporting for the Asia and Pacific at its 34th session in Brasilia, Brazil. All 41 State Parties to the Convention in Asia and the Pacific actively participated in this cycle and worked together on this vital component of

the Convention. The results of the second cycle were presented to the World Heritage Committee at the 36th session in St. Petersburg, Russian Federation during 2012.\textsuperscript{11}

In the Caribbean, States have made progressive steps in creating programmes to combat the destruction and degradation of heritage sites. Capacity Building is one of the key issues in the Region. The lack of management capacity and expertise has been identified by the Latin America and Caribbean Region states as one of the pressing needs that prevents the assurance of better protection for the World Heritage sites in the region. The Caribbean Capacity Building Programme (CCBP) was conceived by the region’s states and endorsed by the World Heritage Committee in 2004. The programme responds to the Latin America and the Caribbean Periodic Report which illustrated how most of the Caribbean States Parties still lack the capacity and expertise needed to enable full protection and management of the present World Heritage sites and to identify new world heritage sites.\textsuperscript{12,13}

The main regions of concern include the Arab States, Latin America and the Caribbean, and Africa. Within the Arab State region, the Taliban destroyed several cultural heritage sites that housed Buddha statues within Afghanistan, blowing the statues up with dynamite.\textsuperscript{14} This included the destruction of more than a dozen Buddha statues in the Kabul museum. The destruction of these artifacts in Afghanistan remains a serious

\textsuperscript{14} Ahmad Rashid, “After 1700 years, Buddhas fall to Taliban dynamite”, The Telegraph, March 12 2001, accessed September 15 2014, \url{http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1326063/After-1700-years-Buddhas-fall-to-Taliban-dynamite.html}. 
concern. Teams from UNESCO as well as the International Committee for Museum Security (ICMS) are engaged in the reconstruction of the destroyed artifacts.\(^\text{15}\)

Sites will retain their “in danger” status until voted on by the World Heritage Committee body to remove sites from the list. For example, as of June 2014, the old city of Jerusalem and its Walls has retained its “in danger” status due to the serious contention in the region. According to the resolution, Jerusalem and its walls, including Al-Magharbeh Gate, are under continuous danger as a result of Israeli policies.\(^\text{16}\) Omar Awadallah, an official in the Palestinian foreign ministry, said that UNESCO originally included the old city of Jerusalem in the list of World Heritage Sites in 1982 after an application filed by Jordan, the declared guardian of the city of Jerusalem. The site has been a main topic for debate during the 38th Session of the WHC. Other endangered sites in the region include the Ancient Cities of Aleppo, Bosra, Damascus, and the Ancient Villages of Northern Syria, all located in the Syrian Arab Republic. These four sites were indicated as heritage sites in danger.\(^\text{17}\)

Sites in danger are not strictly limited to historical or cultural sites, but natural sites as well. Tanzania’s Selous Game Reserve has been listed as a World Heritage Site in Danger in June 2014 due to unprecedented levels of illegal wildlife trade, as announced at the 38th annual World Heritage Committee meeting in Doha, Qatar.\(^\text{18}\) Elephant and rhino poaching triggered by the international demand for ivory and rhino horn, continues


to escalate in Selous, one of the largest remaining wilderness areas in Africa. Also discussed at the meeting in Doha, Australia’s Great Barrier Reef faces a range of threats, including water quality impacts, climate change and proposals for coastal developments. The site will be considered for possible inscription on the World Heritage Danger List in 2015.\(^{19}\) As of the 38th Session of the Committee in 2014, only one World Heritage site listed as being in danger has been removed, United Republic of Tanzania, Ruins of Kilwa Kisiwani and Ruins of Songo Mnara.\(^{20}\)

Another significant issue, aside from cultural landmarks, is the issue of cultural artifacts. Artifacts such as ceramics, artwork, literature, *inter alia*, are often the target of looters and other predation, particularly in combat zones or areas where museums and landmarks are not properly maintained or guarded. Many cultural artifacts disappeared during the 2003 invasion of Iraq, for example. The most troubling and damaging example of this was the looting of the Iraq National Museum in Baghdad during 2003, though a number of other sites in Iraq were damaged and looted as well in the years following the invasion.\(^{21}\) Looters are also known to have targeted artifacts found at landmarks such as the Pyramids at Giza and nearby sites for decades.\(^{22}\)

---


Numerous bodies of the United Nations have been active in addressing the issue of looting. As far back as 1954, the international community adopted the Convention for the Protection of Cultural Property in the Event of Armed Conflict, which obligates states involved in armed conflict to deter looting, and ensure that occupying powers collaborate with local institutions to ensure that cultural artifacts are protected. In 1987, the General Assembly adopted resolution 42/7, which established guidelines for the return of cultural artifacts to their countries of origin. The General Assembly has periodically revised and updated these guidelines as well, most recently by adopting resolution 67/L.34, which additionally calls for awareness-raising and training campaigns, and for states to cooperate with the UN Office on Drugs and Crime (UNODC) and Interpol in combating the trafficking of such artifacts. In 1995, the international community adopted the Convention on Stolen or Illegally Exported Cultural Objects, which provides a claim mechanism for identifying stolen cultural artifacts, while also also protecting the rights of the holders of such stolen property in the event that the object or objects was not known to have been stolen. The Security Council has even been active on the issue of cultural artifacts being stolen or damaged; in 2003 the Security Council adopted Resolution 1483 regarding the Iraq conflict, and included a clause calling for the facilitation of returning artifacts of historical and cultural import to Iraqi control, setting a

precedent for the importance of returning and safeguarding such artifacts in modern conflicts.²⁷

In order to properly address the issue of maintaining and preserving cultural artifacts and landmarks, regions have developed different methods that cater to their specific site requirements, but threats continue to occur within regions ridden by conflict among parties. Each region has unique requirements and means for monitoring and protecting the sites located within their regions. The reporting methods adopted by the World Heritage Committee helps consolidate information and maintain ties to with each state that has taken upon the responsibility of protecting heritage sites within their borders, allowing for the international community to properly address recurring issues and discuss the proper treatment of each site. The instruments adopted by various organs of the United Nations also facilitate awareness-building, preservation campaigns, and training for those directly involved in the protection of artifacts and landmarks. But as the cases of Iraq, Egypt, Jerusalem, Australia, and others indicate, there are still areas in which the existing framework for preservation can be both improved and better applied to ensure that irreplaceable pieces of history are not lost.

Questions to consider:

1. What heritage sites are located in your country and what steps does your country take to preserve said sites?

2. What are the main areas of conflict with cultural and historical landmarks and artifacts? According to your country, which regions or heritage sites require the most attention, if any?

3. What policies has your country or region adopted in regards to cultural tourism? How does tourism affect world heritage sites?

4. How have heritage sites with “in danger” statuses been recovered and preserved in the past?

5. Which organizations has the World Heritage Committee partnered with in the past in order to address world heritage site issues? How have these organizations played a role in actions toward world heritage sites?

6. Is your state a party to instruments such as the Convention on Stolen or Illegally Exported Cultural Objects, the Convention for the Protection of Cultural Property in the Event of Armed Conflict, the Convention Concerning the Protection of the World Cultural and Natural Heritage, among others?
Bibliography


http://triblive.com/ussworld/world/3499557-74/pyramid-egypt-red#axzz3G5RDTdPL.


“List of World Heritage in Danger”.


