LAW IN CONFLICT
THE TECHNOLOGICAL TRANSFORMATION OF WAR AND ITS CONSEQUENCES FOR THE INTERNATIONAL CRIMINAL COURT

LINDSAY FREEMAN*

* Senior Legal Researcher, Human Rights Center, UC Berkeley School of Law. Adv. LL.M. in Public International Law (Leiden University), J.D. (University of San Francisco School of Law), and B.A. in Political Science (Middlebury College); World Economic Forum Global Future Council on Human Rights and Technology fellow and member of the Technology Advisory Board for the Office of the Prosecutor of the International Criminal Court. The views expressed in this article are those of the author and do not reflect the views of any organization. The author thanks Dr. Joseph Powderly and Dr. Alexa Koenig for their guidance, mentorship, and invaluable feedback and the NYU *JILP* team for their editorial support.

Modern armed conflicts and military strategies have undergone dramatic shifts as a result of new technologies, and the next generation of innovations will have profound consequences for how wars are fought, where they are fought, and who fights them. This, in turn, will inevitably have a pronounced influence on the development of the laws of war and the justice mechanisms mandated with enforcing those laws. Therefore, as new strategies and dynamics of war emerge related to the use of new technologies, war crimes investigators and prosecutors must adapt in order to meet the goals of establishing the truth, protecting the historical record, and holding individuals accountable for grave violations of international law. This article examines the characteristics of contemporary armed conflicts related to the use of new technologies and asks how this technological transformation of warfare will affect the ability of the global community to reach the goals of international justice. First, it examines the development of the use of technology—what technologies are used, how they are used, and what impact they have on armed conflicts and military affairs generally. Second, it identifies the complex legal issues arising from the use of new technologies and advocates for needed revisions to the definitions of crimes and modes of liability. Finally, it looks at the impact of the technological transformation of warfare on the fact-finding process for international criminal investigators and recommends a modified approach to evidence and the rules of procedure. In sum, this article takes a big picture approach to examining a current revolution based on the complex interplay of technology, law, and investigations in armed conflicts, and uses this understanding to chart a new way forward for the International Criminal Court.

I. INTRODUCTION

As new technologies transform the character of war,[1] innovative combat strategies and changing dynamics between belligerents will inevitably affect the applicability of the existing laws of war and the ways in which war crimes are investigated and prosecuted. Warfare in the twenty-first century differs greatly from the wars waged during the nineteenth and twentieth centuries—a period during which international humanitarian law formed,[2] paving the way for the creation of sev-

1. As David Jordan and his co-authors explain, "The character of war is a constantly changing phenomenon. It changes depending on upon a number of factors, including the geography of the battlespace, the belligerents and their level of technological development, to name just three. In contrast, the nature of war is unchanging across time and place." DAVID JORDAN ET AL., UNDERSTANDING MODERN WARFARE 49 (2d ed. 2016).

2. As Professors Christine Chinkin and Mary Kaldor describe, "[l]egal steps were first undertaken to reduce war and subsequently to prohibit it after the cataclysm of World War I." CHRISTINE CHINKIN & MARY KALDOR, INTERNATIONAL LAW AND NEW WARS 68 (2017).

eral international war crimes tribunals.[3] The twenty-first century is witness to a rise in internal armed conflicts that are highly internationalized and which transcend borders, blur the line between civil war and civil unrest, and involve numerous fluid groups of non-state actors.[4] These emerging trends can be attributed in large part to the advent and use of new technologies against the backdrop of a changing political landscape. Complicating this picture, the increased importance of the cyber domain makes the informational dimension of warfare often as significant as events on the physical battlefield.[5] Further, the introduction of unmanned vehicles and autonomous systems in military operations are gradually eliminating humans from the decision-making loop. This article examines the characteristics of contemporary armed conflicts related to the use of new technologies and asks how this technological transformation of warfare may impact the global community's ability to reach the goals of international justice.

Technology, science, and war have an entangled history, with the desire for military dominance driving technological innovation, and scientific discoveries propelling warfare to new, previously uncharted frontiers.[6] Within the past century, technological advancements led to the exploitation of air, space, and cyberspace in military operations.[7] Scholars often

---

3. These include the International Military Tribunal at Nuremberg (1945); the International Military Tribunal for the Far East (1946); the International Criminal Tribunal for the former Yugoslavia (1993); the International Criminal Tribunal for Rwanda (1994); the International Criminal Court (1998); the Special Panel for Serious Crimes in East Timor (2000); the Special Court for Sierra Leone (2002); the Extraordinary Chambers in the Courts of Cambodia (2003); the Iraqi High Tribunal (2003); the Special Tribunal for Lebanon (2009); and the Kosovo Specialist Chambers and Specialist Prosecutor's Office (2017).

4. *See* SEBASTIAN VON EINSIEDEL, UNITED NATIONS UNIV. CTR. FOR POLICY RESEARCH, OCCASIONAL PAPER 10, CIVIL WAR TRENDS AND THE CHANGING NATURE OF ARMED CONFLICT (2017) at 2 and 4 (noting global trends in armed conflicts, particularly the rise in civil wars, the increase in conflict relapse rates, the growing number of terrorist and non-state groups, and the internationalization of intrastate conflicts).

5. The United States military refers to cyberspace as the fifth domain of warfare. *See* SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX xix (2014)

6. *See generally* MARTIN VAN CREVELD, TECHNOLOGY AND WAR: FROM 2000 B.C. TO THE PRESENT (1991).

7. JORDAN ET AL., *supra* note 1, at 53.

link fundamental shifts in the conduct of war, sometimes referred to as revolutions in military affairs (RMAs),[8] to the technological developments of the time. In BATTLEFIELD OF THE FUTURE, Jeffrey McKitrick and other scholars explain, "industrialization revolutionized warfare through railroads, the telegraph, the steam engine, rifled guns, and ironclad ships," followed in the interwar period by "blitzkrieg, carrier aviation, amphibious warfare, and strategic bombing."[9] In addition, some less obvious innovations—from the printing press to the internet—have comparably impacted the changing character of war. Therefore, just as the development of sophisticated military technology has undeniably impacted the evolution of armed conflicts, so too have advancements in civilian energy, transportation, and communications technologies. Modern armed conflicts, in particular, have changed dramatically as a result of new digital technologies and their exponentially rapid rate of advancement over the past two decades.[10] However, as P. W. Singer explains in WIRED FOR WAR, the law is not keeping pace with this exponentially rapid rate of technological change.[11]

Technology develops faster than the law.[12] This is especially true of international law. In contrast to the reciprocal relationship between war and technology, and the speed at which both develop, the laws of war progress slowly and somewhat separately. There is a collective hesitation among states regarding cyberspace regulation at the international level, and national lawmakers appear cautious to legislate on issues sur-

8. Jeffrey McKitrick et al., *The Revolution in Military Affairs*, *in* 3 AIR WAR COLL. STUDIES IN NAT'L SEC., BATTLEFIELD OF THE FUTURE: 21ST CENTURY WARFARE ISSUES 65, 65 (Barry R. Schneider & Lawrence E. Grinter eds., 1998) ("A Revolution in Military Affairs (RMA) is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organisational concepts, fundamentally alters the character and conduct of military operations.").

9. *Id.* at 65–66.

10. P. W. SINGER, WIRED FOR WAR 97, 100 (2009).

11. For example, chemical weapons were first used in World War I, but they were not banned by law until eighty-two years later. *Id.* at 387.

12. *See id.* (providing examples of rapid technological evolution and the lack of comparable evolution in the law).

rounding new technologies and technology companies.[13] Further, treaties—which constitute the primary source of international laws of war—take years, if not decades, to form.[14] Even once adopted, treaty law is slow to take hold at the local level—such laws are often difficult to implement and nearly impossible to enforce.[15] As a result, the laws of war have failed to adapt to, address, and keep pace with the reality on the ground.

This disconnect between the law and the reality of modern armed conflicts result from a number of factors, but perhaps the most significant is the dichotomy between the cautious approach of lawyers and the "move fast and break things"[16] mentality of technologists, whose work disrupts societies and norms at unprecedented speeds. There is a trend in legal scholarship to isolate a particular type of technology and theorize about its individual impact on the laws of war, as can be seen in the prolific amount of scholarship focused on the legality of drones in military operations,[17] use of information

13. To date, there has been only one international cyber treaty, which has seen minimal support with only fifty-seven parties. *See* Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185. In addition, as of 2019, there exist very few regulations on social media companies despite their growing power.

14. For example, the establishment of the ICC spans many decades, with initial conversations for a permanent international criminal tribunal beginning after Nuremberg and continuing until the signing of the Rome Statute in 1998. *History of the ICC*, COALITION FOR THE INTERNATIONAL CRIMINAL COURT, http://iccnow.org/?mod=icchistory (last visited Apr. 12, 2019).

15. For example, even over a decade after the entry into force of the Rome Statute, many state parties have not adopted national legislation implementing the key provisions. *Implementing Legislation on the Rome Statute*, PARLIAMENTARIANS FOR GLOBAL ACTION, https://www.pgaction.org/ilhr/rome-statute/implementing-legislation.html (last visited Apr. 12, 2019).

16. This was reportedly the motto of Mark Zuckerberg, CEO of Facebook. *See* Hemant Taneja, *The Era of "Move Fast and Break Things" is Over*, HARV. BUS. REVIEW (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over (attributing the quote to Zuckerberg).

17. *See generally* M.W. Aslam, *A Critical Evaluation of American Drone Strikes in Pakistan: Legality, Legitimacy and Prudence*, 4 CRITICAL STUD. ON TERRORISM 313 (2011); Craig Martin, *A Means–Methods Paradox and the Legality of Drone Strikes in Armed Conflict*, 19 INT'L J. HUM. RTS. 142 (2015); Laurie R. Blank, *After "Top Gun": How Drone Strikes Impact the Law of War*, 33 U. PA. J. INT'L L. 675 (2012).

technologies in network-centric warfare,[18] lethal autonomous systems[19] and cyber warfare.[20] While this siloed approach makes legal analysis more manageable, such division fails to account for how technologies are collectively deployed in and affect the battlefield.

As Singer explains, "the steam engine had to be brought together with everything from railroads to telegraphs for it to culminate as the industrial RMA that shaped World War I."[21] Similarly, fully understanding Germany's Blitzkrieg tactics with an analysis focused only on airplanes would be impossible. During World War II, German forces used tanks and air support, along with communications technologies that integrated the land and air forces.[22] Germany gained competitive advantage over French and British troops, not because it had exclusive access to a particular technology, but because of the way in which German forces used the technologies in concert with each other and integrated them into their overall military strategy.[23] New technologies simply do not operate in isolation. In order to fully understand the current global trends in armed conflict, new technologies must be not only studied independently, but also looked at as a whole.

Another shortcoming in the legal scholarship on technology and warfare is the overemphasis on the obvious, the lethal, and the catastrophic potential outcomes of highly sophisticated military technologies. For example, when the United States and Soviet Union made technological advancements in

---

18. *See generally* DAVID S. ALBERTS ET AL., NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (2d rev. ed. 2000).

19. *See generally* ARMIN KRISHNAN, KILLER ROBOTS: LEGALITY AND ETHICALITY OF AUTONOMOUS WEAPONS (2009); Heather M. Roff, *The Strategic Robot Problem: Lethal Autonomous Weapons in War*, 13 J. MIL. ETHICS 211 (2014); Peter Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision–Making*, 94 INT'L REV. RED CROSS 687 (2012).

20. As UNDERSTANDING MODERN WARFARE explains, "Akin to the strategic bombing literature, cyberwar discourse overly simplifies the complex, multidimensional, polymorphous activity of strategy. It assumes too readily that strategic success can be reduced to tactical performance in one field of activity." JORDAN ET AL., *supra* note 1, at 70.

21. SINGER, *supra* note 10, at 193.

22. McKitrick, *supra* note 8, at 65–66 (noting the blitzkrieg was accompanied by carrier aviation, amphibious warfare and strategic bombing).

23. *Id.*

space exploration in the 1960s, legal commentaries focused heavily on the fear of nuclear weapons and the militarization of space,[24] rather than on understanding the consequences of communications satellites, which have a significant impact on military operations. Similarly, academic writings today concentrate principally on catastrophic cyber warfare or lethal autonomous weapons,[25] rather than on the significantly more pervasive and detrimental cyber invasions[26] or on the legal and ethical implications of non-lethal autonomous systems and their use in strategic planning. As a result of prioritizing high technologies designed for military purposes and their worst-case scenarios over the more pervasive and far-reaching use of civilian technologies in armed conflicts, legal scholarship often overlooks and underappreciates a number of everyday technologies and their influence on the evolution of military affairs. This article fills that gap by also addressing the subtler, yet arguably more significant impact of common civilian technologies.

The next generation of military and civilian technologies, which include numerous recent breakthroughs in the fields of robotics, autonomous systems, encryption, machine learning, and artificial intelligence, will have profound consequences for how wars are fought, where they are fought, and who fights them. This, in turn, will inevitably influence the development of the laws of war and the justice mechanisms mandated with enforcing those laws. The diverse actors entering the physical

---

24. *See, e.g.*, Allan Rosas, *The Militarization of Space and International Law*, 20 J. PEACE RES. 357, 357 (1983) ("During recent years it has become apparent that space is an important theater for the military activities and aspirations of the great powers."); David H. Small, *Security Aspects of the Current United Nations Space Law Agenda*, 11 J. SPACE L. 51 (1983) (discussing core issues raised by military use of outer space within the context of UN processes); Marko G. Markoff, *Disarmament and "Peaceful Purposes" Provisions in the 1967 Outer Space Treaty*, 4 J. SPACE L. 3 (1976) (discussing military activities in outer space in the context of the 1967 Outer Space Treaty).

25. As David Sanger explains, "[w]e have spent so much time worrying about a 'cyber Pearl Harbor,' the attack that takes out the power grid, that we have focused far too little on the subtle manipulation of data that can mean that no election, medical record or self-driving car can be truly trusted." David E. Sanger, *Why Hackers Aren't Afraid of Us*, N.Y. TIMES (June 16, 2018), https://www.nytimes.com/2018/06/16/sunday-review/why-hackers-arent-afraid-of-us.html.

26. *Id.*

and cyber battlefields make application of the traditional international humanitarian law's classifications increasingly difficult for lawyers. Further, the speed and openness of information exchange, the vast and growing volume of data, and the ease with which digital material can be manipulated or distorted, frustrates the ability of war crimes investigators to ferret out the truth. Therefore, an updated and more flexible legal framework that takes into account how technologies are transforming armed conflicts in the twenty-first century is sorely needed.

This article argues that the international criminal justice system, centered around the International Criminal Court (ICC), offers a suitable framework—so long as investigators, lawyers, and judges keep pace with real world developments and interpret the law accordingly. This article further identifies and analyzes the most likely potential challenges for international criminal law practitioners based on the technological transformation of warfare. First, it examines how the use of technology in conflict is taking effect—what technologies are used, how are they used, and what impact they have on armed conflicts and military affairs generally. Second, it identifies several complex legal issues related to the use of new technologies in armed conflicts and advocates for a fresh approach to thinking about international crimes and individual criminal responsibility. Finally, it considers how the use of information and communications technologies (ICTs) in modern conflicts impacts the fact-finding process for war crimes investigators. It identifies new opportunities for collecting evidence in a changing information environment and assesses the adequacy of existing evidentiary and procedural rules to address emerging challenges associated with the digitalization of evidence. In sum, this article takes a big picture approach to explain a current revolution based on the complex interplay of technology, law, and fact-finding in armed conflicts and uses this broader understanding to chart a new way forward for the ICC.

II. Understanding the Technological Transformation of War

There are a number of military theories and terms used to understand and describe the changing character of warfare.

From Sun Tzu[27] to Carl von Clausewitz[28] to Che Guevara,[29] military theorists often espouse concepts and principles of war strategy and of military affairs. In the modern era, the number of theorists and theories has multiplied. This proliferation may be attributed to the expansion of information fora and publications dedicated to understanding war, as well as the broadening of interested actors. With the development of international humanitarian law (IHL)[30] and international criminal law (ICL) as fields of practice,[31] more and more lawyers weigh in on the quest of understanding and characterizing warfare.

With the signing of the 1977 Additional Protocols to the Geneva Convention of 1949, member states prescribed two classifications of war: international armed conflict (IAC) and non-international armed conflict (NIAC).[32] Article 8 of Rome Statute of the ICC, which was signed in 1998 and entered into force in July 2002, adopted these binary categories.[33] While

27. *See* SUN TZU, THE ART OF WAR (Samuel B. Griffith trans., Oxford Univ. Press 1963).

28. *See* CARL VON CLAUSEWITZ, ON WAR (Michael Eliot Howard & Peter Paret eds. &trans., Princeton Univ. Press 1989).

29. *See* CHE GUEVARA, GUERRILLA WARFARE (SR Books 3rd ed. 1997).

30. As explained in a leaflet about the ICC Moot Competition, "IHL is a branch of public international law that regulates the conduct of hostilities (*jus in bello*). . . . It applies from the moment armed conflicts are initiated and extends beyond the cessation of hostilities, until a general conclusion of peace has been reached." Andy Niv, *IHL, ICL and the ICC in a Glimpse*, ASS'N FOR THE PROMOTION OF INT'L HUMANITARIAN LAW, http://iccmoot.com/wp-content/uploads/2016/11/IHL-ICL-and-the-ICC-in-a-glimpse-Ady-Niv.pdf (last visited Mar. 22, 2019).

31. The same leaflet describes ICL as "a branch of public international law that concerns the criminal responsibility of individuals for international crimes . . . [W]ar crimes originate in IHL, whereas genocide and crimes against humanity find their origins in international human rights law." *Id.*

32. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287 [hereinafter Fourth Geneva Convention]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol II].

33. Rome Statute of the International Criminal Court art. 8.2(b)–(c), July 17, 1998, 2187 U.N.T.S. 3 [hereinafter Rome Statute] (articulating a list of "violations of the laws and customs applicable in international armed conflict," and providing a separate list for "case[s] of an armed conflict not of an international character.").

IAC and NIAC are legal terms, it is interesting to observe the quantity of new terms that have emerged since the Additional Protocols to describe modern armed conflicts. This list includes, but is not limited to: guerilla warfare, unconventional warfare, asymmetrical warfare, irregular warfare,[34] fourth generation warfare,[35] hybrid warfare,[36] network-centric warfare,[37] information warfare, insurgency and counterinsurgency, terrorism and counterterrorism, new wars, political wars, proxy wars, extra-state wars and internationalized wars.[38]

As evinced by the myriad characterizations, war has always had a "polymorphous character," taking on a number of different forms.[39] However, the pace of technological development and the rise of insurgencies and terrorism in the contemporary era have created a profoundly complex operational environment.[40] This complex environment has led numerous scholars to attempt to identify patterns and develop new theo-

34. *See* SINGER, *supra* note 10, at 213 ("Much of war is no longer battles between equally matched state armies in open fields, but rather 'irregular warfare,' that amalgam of counterinsurgency, counterterrorism, peace, stability, and support operations.").

35. Fourth generation of warfare is characterized by "a return to decentralized forms of warfare, blurring of the lines between war and politics, combatants and civilians due to nation states loss of their near-monopoly on combat forces, returning to modes of conflict common in pre-modern times." Steven Rosefielde, *Great Powers Resurgence*, *in* THE UNWINDING OF THE GLOBALIST DREAM: EU, RUSSIA AND CHINA 113, 129 (Steven Rosefielde et al. eds., 2018).

36. In the context of military confrontation, a hybrid threat has been described as one that "simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battle space." Brian P. Fleming, *Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art* (U.S. Army Command & Gen. Staff Coll., Monograph, 2011).

37. Network-centric warfare describes the effect that the introduction of new information technologies such as computers, the Internet, and fiber optics had on the strategy of war. Network centric-operations use information technology and computer networks to coordinate geographically dispersed troops, in manner mimicking decentralized terrorist networks. *See generally* Arthur K. Cebrowski & John H. Garstka, *Network-Centric Warfare: Its Origin and Future*, 124 PROC. 139 (1998).

38. *See* CHINKIN & KALDOR, *supra* note 2, at 6 (discussing meaning and use of the term "new wars.").

39. JORDAN ET AL., *supra* note 1, at 45.

40. *Id.* at 53 ("from an operational perspective the modern era has undoubtedly produced a more complex environment.").

retical frameworks to better understand contemporary armed conflicts. This section discusses some of these theories and observed trends in contemporary wars through analysis of recent and ongoing armed conflicts in Afghanistan, Iraq, Libya, Syria, Yemen, Mali, South Sudan, Somalia, Central African Republic (CAR), Democratic Republic of Congo (DRC), the Israeli/Palestinian territories, and eastern Ukraine. This section also seeks to understand the root causes of these trends by examining the role new technologies play in modern conflicts.

A. *Theoretical Frameworks*

While scholars today espouse many military theories when discussing recent changes in warfare, this article focuses on two pertinent theories concerning the impact of technology on the evolving character of war: (1) the revolution in military affairs (RMA) theory and (2) the new wars theory.[41] The RMA theory describes paradigm shifts in the waging of war as connected to technological and organizational shifts in military strategy.[42] An RMA is "a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations."[43] As Steven Metz and James Kievit recount, "[t]he notion of military revolutions grew from Soviet writing in the 1970s and 1980s. Early studies talked of a 'military technical revolution' (MTR), but this quickly evolved into the more holistic concept of revolutions in military affairs.[44] This theory sees wars in Iraq and Afghanistan as hallmarks of the current RMA, where new technologies led to new philosophies about how to beat irregular enemies using a network-centric model with smaller teams

41. *Id.* at 129, 132.

42. McKitrick et al., *supra* note 8, at 65.

43. *Id.* For further discussion of the concept of RMA, see generally Lothar Ibrügger (General Rapporteur, Science and Technology Committee, NATO Parliamentary Assembly), *The Revolution in Military Affairs* (Nov. 1998), http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html.

44. Steven Metz & James Kievit, Strategy and the Revolution in Military Affairs: From Theory to Policy v (1995).

of decentralized forces and targeted killings by remote operators.[45]

In contrast, the new wars theory, as reflected in the writings of professors Mary Kaldor and Christine Chinkin, as well as Herfield Munkler and General Sir Rupert Smith, sees geopolitical change as the cause of new wars.[46] In INTERNATIONAL LAW AND NEW WARS, Kaldor and Chinkin describe new wars as "instances of armed conflict and violence in places such as Syria, Ukraine, Libya, Mali, the Democratic Republic of Congo and South Sudan."[47] New wars are characterized by fighting between "varying combinations of networks of state and non-state actors," among other factors.[48] Instead of focusing on high technology used by state militaries, these scholars view contemporary conflicts as "almost neo-medieval in character," describing them as "brutal, local and decidedly low-tech."[49]

Analysts and academics describe the RMA and new wars theories in contrast to one another, but both theories come to essentially the same conclusion: technological innovation plays a role in changing the character of armed conflict. The contrast stems from the fact that the RMA theory focuses on the use of high technology by professional militaries and a conscious choice to adapt strategy to incorporate innovations, whereas the new wars theory focuses on the skilled exploitation of everyday technology by non-state networks whose use of the technology organically leads to new operational strategies. New wars theorists see globalization as the driving force changing warfare rather than technology, although they acknowledge technology has impact on globalization. Thus, the conception of new wars is as tied to technological change as the RMA theory. These two theoretical models reveal that technol-

---

45. *See generally* Alexander Salt, *Transformation and the War in Afghanistan*, STRATEGIC STUD. Q., Spring 2018, at 98; Henrik Olsen Nordal, Thinking of Revolution in Military Affairs (RMA): Towards a Common Understanding of RMA (Nov. 20, 2013) (unpublished Master's thesis, Universitetet i Oslo), https://www.duo.uio.no/bitstream/handle/10852/39902/Thinking-of-RMA—Master-of-Philosophy-thesis-by-Henrik-O—Nordal-.pdf?sequence=1.

46. JORDAN ET AL., *supra* note 1, at 132 ("For the 'new wars' school, the driving force in shaping future warfare is not military technology but the process of globalisation.").

47. CHINKIN & KALDOR, *supra* note 2, at 3.

48. Mary Kaldor, *In Defence of New Wars*, STABILITY, Mar. 7, 2013, at 1, 2.

49. JORDAN ET AL., *supra* note 1, at 132.

ogy must be understood at all levels and in all its forms, in all parts of society and geopolitics, in order to comprehend this new state of military affairs. Achieving a higher understanding of modern military affairs also requires moving away from theoretical frameworks towards an analysis of practical, real-world impact, as developed in the following sub-sections.

B. *Characteristics of Twenty-first Century Conflict*

In the eighteenth and nineteenth centuries, the rise of nation-states led to the professionalization of the military. The Western idea of the state and state sovereignty, which emerged in the Westphalian era[50] and later received recognition in the United Nations Charter,[51] was closely tied to control over the use of force.[52] However, as Singer explains, "[w]ith the rise of globalization in the twenty-first century, these old ideas of a nation-state and its uniformed military are transforming."[53] Over the past few decades, as journalist David Patrikarakos notes, the world has seen a "decline in state-on-state conflict and an almost total absence of (direct) war between two major powers."[54]

War is no longer carried out exclusively by states, but also by non-state actors who are not bound by the laws of war in the same way as the states for which they were designed.[55] While tribalism, terrorism, and insurgencies date back hundreds of

---

50. The Treaty of Westphalia, which some mark as the beginning of international law, was concluded in 1648 after the Thirty Years' War. *Treaty of Westphalia*, ELECTRONIC INFO. SYS. INT'L L., http://www.eisil.org/index.php?sid=4ails&id=658&t=link_details&cat=520 (last visited Mar. 22, 2019).

51. U.N. Charter art. 2, ¶¶ 1–5.

52. TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 3 (2018) ("[T]he idea of a monopoly over the legitimate use of force is very much linked to the European experience of the emergence of the nation-state and the Westphalian notion of sovereignty that became codified globally after World War II through the Charter of the United Nations.").

53. SINGER, *supra* note 10, at 362.

54. DAVID PATRIKARAKOS, WAR IN 140 CHARACTERS: HOW SOCIAL MEDIA IS RESHAPING CONFLICT IN THE TWENTY–FIRST CENTURY 6 (2017).

55. Cedric Ryngaert, *Non-State Actors and International Humanitarian Law* 4 (Institute for International Law Working Paper, 2008), https://www.law.kuleuven.be/iir/nl/onderzoek/working-papers/WP146e.pdf ("statements that non-State armed groups are bound by IHL do not solve this major conceptual problem with undesirable practical repercussions: how can insurgent groups be bound by IHL conventions which they have not signed up to?").

years, emerging ICTs such as smartphones and the internet allow non-state groups to communicate, organize, and operate on a parallel plane to states in ways never seen before. As Patrikarakos describes, "[f]rom Iraq to Syria to Gaza, government militaries are forced to fight adversaries who place themselves within the civilian arena."[56] Similarly, Singer explains that "[s]tates across the globe are increasingly involved in violent conflicts with non-state groups within and across borders."[57] Many ongoing conflicts involve multiple parties with asymmetry between their power and resources.[58] With the increased involvement of non-state actors comes a lack of clarity over whether certain actions taken in the name of counterterrorism qualify as acts of war or international policing.

Another factor that distinguishes contemporary armed conflicts between states and non-state actors from wars of the past is how these groups organize and operate. Unlike states, which are for the most part established entities, non-state groups are not stable organizations with fixed members, but vary greatly over time. Accordingly, in many ongoing armed conflicts there is multiplicity,[59] fluidity,[60] and fragmentation[61]

---

56. PATRIKARAKOS, *supra* note 54, at 73.

57. SINGER, *supra* note 10, at 95.

58. JAHANGIR ARASLI, INEGMA SPECIAL REPORT NO. 13, STATES VS. NON–STATE ACTORS: ASYMMETRIC CONFLICT OF THE 21ST CENTURY AND CHALLENGES TO MILITARY TRANSFORMATION (2011), http://www.inegma.com/Admin/Content/File-81020131379.pdf.

59. Multiplicity refers to a large number. *Multiplicity*, MERRIAM–WEBSTER, https://www.merriam-webster.com/dictionary/multiplicity (last visited Mar. 22, 2019).

60. Fluidity refers to continuous, amorphous properties. *Fluidity*, MERRIAM–WEBSTER, https://www.merriam-webster.com/dictionary/fluidity (last visited Mar. 22, 2019). For example, since the Syrian war began in 2011, the Syria Mapping Project at the Carter Center has tracked the formation and dismantling of over 7,000 armed groups. See *Syria Conflict Resolution*, CARTER CTR., https://www.cartercenter.org/syria-conflict-map/ (last visited Mar. 22, 2019) (describing the mapping project and providing periodic conflict summary reports dating back to 2013).

61. Fragmentation refers to process of breaking into fragments or smaller groups. *Fragmentation*, MERRIAM–WEBSTER, https://www.merriam-webster.com/dictionary/fragmentation (last visited Mar. 22, 2019); *see also Fragment*, MERRIAM–WEBSTER, https://www.merriam-webster.com/dictionary/fragment (last visited Mar. 22, 2019). For further discussion of fragmentation in conflict, see generally KATHLEEN GALLAGHER CUNNINGHAM, OSLO FORUM PAPERS NO. 6, UNDERSTANDING FRAGMENTATION IN CONFLICT AND ITS IMPACT ON PROSPECTS FOR PEACE (Dec. 2016), https://www.hdcentre.org/

between various armed groups. As Nathalie Durhin suggests, modern wars not only involve multiple armed groups, but the membership of those groups frequently shifts throughout the course of the conflict.[62] In Syria, for example, those documenting the conflict tracked the formation, and in many cases the collapse, of over seven thousand armed groups since conflict began in 2011.[63] The DRC provides another example in which the proliferation of armed groups and fragmentation led to more than sixty distinct armed groups operating in one conflict.[64] Similar trends are visible in Yemen[65] and Libya.[66] Fragmentation also appears on the international stage, where discrete jihadist groups—including the Islamic State in Iraq and Syria (ISIS), al-Nusra in Syria, Al-Saiqa in Libya, Ansar Dine in Mali, and Boko Haram in Nigeria—find their origins in al-Qaeda.[67]

In addition to new actors, the strict territoriality of the wars of the past is transformed by foreign involvement in internal conflicts and the decreasing importance of physical borders. Since the turn of the millennium, there has been a rise in chaotic civil armed conflicts without clear temporal or geo-

---

wp-content/uploads/2017/02/Understanding-fragmentation-in-conflict.pdf.

62. Nathalie Durhin, *Protecting Civilians in Urban Areas: A Military Perspective on the Application of International Humanitarian Law*, 98 INT'L REV. RED CROSS 177, 183 (2016) (recounting the need for armed forces to gather up-to-date intelligence about the membership of armed groups, and describing how this plays out in the conflict against Daesh in the Levant).

63. *See Tracking the Front Lines in Syria*, THE CARTER CTR., https://d3svb6mundity5.cloudfront.net/dashboard/index.html (last visited Feb. 21, 2019) (providing an interactive map that shows the evolution of the Syrian conflict over time, based on the groups controlling territory).

64. JASON K. STEARNS & CHRISTOPH VOGEL, CONGO RESEARCH GRP., THE LANDSCAPE OF ARMED GROUPS IN THE EASTERN CONGO 4 (2015) (providing a map of the armed groups in North and South Kivu as of October 2015).

65. LOUISE ARIMATSU & MOHBUBA CHOUDHURY, THE LEGAL CLASSIFICATION OF THE ARMED CONFLICTS IN SYRIA, YEMEN AND LIBYA 20–33 (2014) (detailing the complex legal arguments and open debate on how to characterize the conflict in Yemen).

66. *Id.* at 34–41, 42 (detailing the legal arguments on how to characterize the Libyan conflict and reaching the conclusion that more research is necessary).

67. Frank Gardner, *Jihadist Groups Around the World*, BBC NEWS (June 19, 2014) https://www.bbc.com/news/world-middle-east-27930414.

graphic boundaries.[68] In addition, the amorphous war on terror left its mark on a number of territories, with no clear end in sight or defined criteria for victory. Further, many recent conflicts occur on the territory of weak or failing states and result in surges of refugee flows onto neighboring territories. Examples cited in the United Nations University Centre for Policy Research report include Afghanistan, Libya, South Sudan, and Ukraine.[69] Central to these changes is also the blurring line between internal violence and international armed conflict[70] and, as Emile Simpson points out, "blurring the conceptual boundaries between war and peace."[71] Social media, Simpson explains, "blurs the beginning and end of a war because the informational dimension can start long before active combat and continue long after battlefield operations have finished."[72] The cyber dimension of many modern conflicts also exacerbates the lack of clear geographical and temporal boundaries.

The number of major civil wars has tripled over the past two decades, and these conflicts are increasingly convoluted.[73] While civil wars are not new, their international impact and the degree of involvement and influence by external actors is unlike situations in the past. Many recent conflicts are internal yet involve external military interventions or the use of foreign fighters.[74] For example, the ISIS contingent in Syria is made up in large measure of foreign fighters,[75] a phenomenon ap-

68. *See generally* EINSIEDEL, *supra* note 4, at 2 (discussing the rise in the number of civil wars and intrastate conflicts since the early 2000s).

69. *Id.* at 3.

70. PATRIKARAKOS, *supra* note 54, at 259 (discussing the role of social media networks, inherently "not built around the architecture of a single state," in the rise of the Islamic State, and how that group's movement is premised on the destruction of the nation state).

71. EMILE SIMPSON, WAR FROM THE GROUND UP: TWENTY-FIRST CENTURY WAR AS POLITICS 9 (2013).

72. PATRIKARAKOS, *supra* note 54, at 259 (discussing Simpson's beliefs).

73. *Id.*

74. *See generally* Kristian Skrede Gleditsch, Idean Salehyan & Kenneth Schultz, *Fighting at Home, Fighting Abroad: How Civil Wars Lead to International Disputes*, 52 J. CONFLICT RESOL. 479 (2008) (discussing the interplay between internal and external conflicts).

75. BÉRÉNICE BOUTIN ET AL., INTERNATIONAL CENTRE FOR COUNTER-TERRORISM, THE FOREIGN FIGHTERS PHENOMENON IN THE EUROPEAN UNION 3 (Bibi van Ginkel & Eva Entenmann, eds. 2016), https://icct.nl/wp-content/

parently possible due to social media.[76] Research shows that terrorist groups use social media and mobile applications such as Viber and WhatsApp as recruitment tools for foreign fighters to Syria from other countries in North Africa and the Middle East.[77] As Patrikarakos reports, "more foreign fighters have gone to Syria, most of them to join Islamic State, than went to fight in Iraq when American troops invaded or in Afghanistan during the decade-long Soviet-Afghan war. This simply cannot be explained without the recruiting power of social media."[78]

This surge in foreign fighters joining battles abroad through non-traditional and unofficial recruitment channels complicate the threshold issue of characterizing the conflict—particularly whether it is IAC or NIAC. In circumstances where conflicts are borderless or internationalized, compelling and conflicting arguments exist concerning the appropriate label for the conflict. Distinguishing between these binary categories was far easier at the time of creation of the classifications, but the analysis is exceedingly difficult in the twenty-first century. Today, a growing number of conflicts between states and non-state actors are outside their territory or involve foreign fighters—a challenge for international law explained and expanded on below.

C. *The Nature of Technological Change*

While these changes in the actors and geographic scope of armed conflicts result from a number of factors, at the core of the changes is modern technological development and the ways in which digital technologies shift power from states to non-state actors. As noted earlier, the analysis in this article is not focused on a specific technology, but rather aims at understanding the social, cultural, economic, and political changes that occur as a result of many new technologies. This section examines the overarching characteristics of technology to better understand the changes in armed conflicts.

---

uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_1-April-2016_including-AnnexesLinks.pdf.

76. *See id.* at 54–55 (discussing the role of social media as a powerful instrument where many recruits are first targeted).

77. PATRIKARAKOS, *supra* note 54, at 209.

78. *Id.*

Technology is developing at an exponentially rapid pace, a phenomenon observable through a variety of modern innovations, particularly cell phones and computers.[79] There is a factual basis for the overwhelming feeling of the increased speed of technological change, which Singer refers to as Moore's law, named after the co-founder of Intel. Moore observed that the number of transistors on a microchip was roughly doubling every two years.[80] Singer provides the striking case in point: "[t]he current rates of doubling mean that we experienced more technologic change in the 1990s than the entire ninety years beforehand."[81] Therefore, while past generations had decades to digest each new invention, the current generation has years or months.[82] Computers are also exponentially more powerful and at the same time smaller and cheaper. Other examples cited by Singer include: "[w]ireless capacity doubles every nine months. Optical capacity doubles every twelve months. The cost/performance ratio of Internet service providers is doubling every twelve months. Internet bandwidth backbone is doubling roughly every twelve months." Further, as technology advances, costs drop, and lower costs lead to increased market penetration.[83] Due to these changes, non-state actors now have the capacity to conduct activities once thought to be in the sole purview of states—like disseminating propaganda to a broad audience or attacking the infrastructure of a sovereign state. Many technologies developed for military purposes now reside in the civilian sphere,[84] and the time lapse between the costly develop-

79. In WIRED FOR WAR, Singer provides numerous concrete examples of technologies that are developing at exponential pace. *See* SINGER, *supra* note 10, at 98–99.

80. *Id.* at 97–98.

81. *Id.* at 101.

82. *Id.*

83. *Id.* at 99.

84. *See, e.g.*, Ben Yunmo Wang, Nathaniel A. Raymond, Gabrielle Gould & Isaac Baker, *Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities*, STABILITY, Oct. 22, 2013, at 1, 1 ("Changes to US law and policies in the 1990s allowed private companies to provide satellite imagery to a broader range of actors. This development enabled non-governmental actors . . . to acquire previously classified geospatial imagery and task private satellites to collect new imagery.").

ment of military technologies by private contractors and their inevitable falling into the public domain is shrinking.[85]

The exponential rate of change strongly impacts the sharing of information today, as well as the connections among technological developments across disciplines. Singer explains that "advancements in one field feed advancements in others. And lower prices in one field help feed new development in others."[86] For example, advances in neuroscience and brain mapping led to the development of artificial neural networks modeled after biological neural structures, which in turn led to advancements in machine learning and big data analysis.[87] Similarly, advances in the field of physics are central to quantum computing, which theoretically could generate the computing power necessary to realize artificial general intelligence.[88] Thus, another feature of modern technologies brought about by the internet and the mobility and affordability of mobile digital devices, is the speed, volume, and openness of information.

Social media empowers individuals to broadcast a message and circulate it to wide audiences "at unprecedented

---

85. In 1983, DARPA invented miniaturized GPS receivers. *Miniaturized GPS Receivers*, DEF. ADVANCED RES. PROJECTS AGENCY, https://www.darpa.mil/about-us/timeline/miniaturized-gps-receivers (last visited Mar. 22, 2019). In 1989 the Magellan Corporation marketed hand-held navigation devices in the U.S. *See* Mark Sullivan, *A Brief History of GPS*, PCWORLD (Aug. 9, 2012, 7:00 A.M.), https://www.pcworld.com/article/2000276/a-brief-history-of-gps.html.

86. SINGER, *supra* note 10, at 99.

87. Different scientific reports support parts of this proposition. *Compare* KEVIN GURNEY, AN INTRODUCTION TO NEURAL NETWORKS (1997) *with* Nicola Bernini, *Artificial Neural Networks and Neuroscience*, TOWARDS DATA SCI. (Apr. 25, 2017), https://towardsdatascience.com/artifician-neural-networks-and-neuroscience-e4852b10d7a9.

88. George Musser, *Job One for Quantum Computers: Boost Artificial Intelligence*, QUANTA MAG. (Jan. 29, 2018), https://www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/ ("Given a big enough and fast enough quantum computer, we could revolutionize many areas of machine learning."); Bernard Marr, *How Quantum Computing Will Revolutionize Artificial Intelligence, Machine Learning and Big Data*, FORBES (Sept. 5, 2017), https://www.forbes.com/sites/bernardmarr/2017/09/05/how-quantum-computers-will-revolutionize-artificial-intelligence-machine-learning-and-big-data/ ("It's predicted that artificial intelligence, and in particular machine learning, can benefit from advances in quantum computing technology . . . .").

speeds."[89] As a result, governments and media outlets lost their monopoly over information distribution and content creation.[90] The lower barriers to entry are related not just to the declining cost of certain technologies, but also to the availability of information. With the pervasiveness of today's digital technologies, "the spread of knowledge is nearly instantaneous."[91] The internet also facilitates distribution of open source software, code, algorithms, and other technical information. Consequently, developers build off of each other's past accomplishments, further accelerating change.[92] This ubiquitous access to information levels the playing field and shifts power from states to non-state actors such as organized armed groups, multinational corporations, international organizations, and even individuals.

ICTs—which include the internet, smartphones, and satellites—have improved global connectivity in political, cultural, and economic life. Militaries, organized armed groups, and individuals in conflict zones use these technologies for a range of purposes, but particularly to recruit, organize, network, and plan.[93] Social media platforms, in particular, facilitate the ability of networks of individuals to coalesce around issues or ideas. This dynamic is reflected in ongoing conflicts, where networks form around extremist or opposition movements. The Arab Spring is a cogent and frequently cited example of this phenomenon.[94] Such networks cannot be con-

89. PATRIKARAKOS, *supra* note 54, at 50 (illustrating this effect by recounting the 2010 Gaza flotilla raid).

90. *Id.* at 46.

91. SINGER, *supra* note 10, at 100.

92. *See id.* at 270 ("'[D]o it yourself'" kits are making robots accessible to just about anyone, including systems with capabilities that were just a few years ago considered military grade.").

93. *See* U.N. Office on Drugs & Crime, *The Use of the Internet for Terrorist Purposes*, at 3 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (identifying six categories of means by which the internet is used to promote terrorism); Jytte Klausen, *Tweeting the* Jihad*: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, 38 STUD. CONFLICT & TERRORISM 1, 1 (2015) (reporting on a study of the means by which Western foreign fighters used Twitter "feeder accounts" to proselytize and recruit); ZEYNEP TUFEKCI, TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTESTS (2017) (discussing the Arab Spring and internet-fueled social movements).

94. *See generally* TUFEKCI, *supra* note 93.

trolled by the state or insulated territorially.[95] As a result of their enhanced ability to communicate and coordinate, non-governmental organizations (NGOs) and social movements are increasingly important and have growing international influence.[96] As Kaldor and Chinkin explain, "[t]he dramatic expansion of the internet, mobile telephony and social media underpins the proliferation of global networks at and across all levels of society."[97] This new reality has, in essence, enabled and emboldened the formerly powerless and disenfranchised by amplifying their voices and allowing them to mobilize as never before.[98] These characteristics of technological change and the corresponding trends in contemporary armed conflicts illustrate just how dramatically differently warfare operates today than when the ICC began its operations nearly twenty years ago. Exploration of whether the laws created before this period hold up in today's context is vitally important.

III. TECHNOLOGY IN CONFLICT

New technologies have caused a tectonic shift in global power, as the authority and control of states—particularly in terms of their monopoly on the use of force—dwindled and the power of non-state actors, private entities, and individual citizens rose.[99] Modern armed conflicts reflect this shift in power. As Singer articulates, "the state's monopoly on protection and violence is challenged by non-state groups, terrorist

95. *See* CHINKIN & KALDOR, *supra* note 2, at 61 (discussing the emergence of "global civil society" that transcends national boundaries and is assisted by technology).

96. *See id.* at 58 (discussing "the growing role of non-state actors in upholding international norms.").

97. *Id.*

98. Social media's power to transcend the internet and affect real-world change is perhaps most apparent in the Arab Spring movement. *See* PATRIKARAKOS, *supra* note 54, at 92, 133 (describing the role of social media in enabling and catalyzing the Arab Spring and other opposition movements).

99. Elke Krahmann, *Private Security Companies and the State Monopoly on Violence: A Case of Norm Change?* 1, 26 (PRIF Reports Working Paper 88, 2009) (examining whether there is evidence of changing norms around the state monopoly on armed force and concluding that "this norm appears to be put into question by the proliferation of private security contractors").

networks, and even individuals, all empowered with dangerous new technologies."[100]

After the first World War, humanity witnessed a dramatic growth in interconnectedness, which, as Kaldor and Chinkin describe, had "a profound impact on the actual character of states."[101] As this interconnectedness grew in the post-World War II period, international organizations like the United Nations (UN) and global lawmaking flourished. Until the mid-twentieth century, states were the only recognized entities operating as legal persons at the international level. Then, in 1949, the International Court of Justice issued an advisory opinion determining that the UN is a subject of international law, enjoying objective international legal personality.[102] International scholars and lawmaking bodies soon accepted that this legal personality extended to other international institutions as well.[103] Globalization also facilitated the possibility of large, multinational corporations eventually rising to international legal person status.[104] Consequently, this increased interconnectedness led to what Kaldor and Chinkin characterize as "the recognition that a wider range of actors exercise power on the international plane," including individuals, international organizations, NGOs, and multinational corporations.[105]

A. *Rise of the Non-State Actors*

Today, states are no longer the only actors participating in and influencing global politics and the international legal order. This decentralization and flattening of power structures is not only happening at the international level, but also within various organizations and entities.[106] The traditional hierar-

---

100. SINGER, *supra* note 10, at 278.

101. CHINKIN & KALDOR, *supra* note 2, at 56.

102. Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. Rep. 174, 179 (Apr. 11).

103. CHINKIN & KALDOR, *supra* note 2, at 56.

104. Tara Van Ho, *International Legal Personality of Corporations: How Investment Law Answers the Supreme Court Question in Jesner*, JUST SECURITY (Oct. 2, 2017) https://www.justsecurity.org/45543/international-legal-personality-corporations-investment-law-answers-supreme-court-question-jesner/.

105. CHINKIN & KALDOR, *supra* note 2, at 61.

106. For example, in an analysis of Google's organizations structure, Nathaniel Smithson highlights the company's emphasis on "flatness." Nathaniel

chies and bureaucracies of governmental, public, and private entities are all disrupted by technology. This is even true of militaries, the epitome of hierarchical command structures.[107] In response to the challenge of irregular forces such as terrorists, insurgents, and guerillas, some militaries are adapting their strategies to beat new foes by being equally flexible, flattened, and decentralized.[108] This section describes how various types of non-state actors are playing increasingly important roles in contemporary armed conflicts and how their use of new technologies blurs the line between civilians and combatants.

The new millennium is witness to a growth in multinational corporations with revenues that rival the GDP of midsize countries and a consequent financial redistribution that locates much of the world's wealth in the private sector.[109] One of the prominent trends in twenty-first century warfare is the increased use of private corporations to develop weapons and equipment; provide administrative, logistical, and tactical support; and, most significantly, supply private forces or mercenaries.[110] The use of mercenaries in warfare is not a new phenomenon, but its reemergence in the modern era raises provocative legal issues.[111] The line between private entities and

---

Smithson, *Google's Organizational Structure & Organizational Culture (An Analysis)*, PANMORE INST. (Feb. 13, 2019), http://panmore.com/google-organizational-structure-organizational-culture.

107. *See* Michael Kometer, *The Strategy of Control: Centralized vs. Decentralized Control of US Airpower*, 3 DEF. STUD. 63 (2003) (discussing the U.S. military's move towards, and experimentation with decentralized forces).

108. *Cf. id.* at 36 (discussing the U.S. military's application of network centric warfare during the 2003 Iraq War).

109. As Jed Greer and Kavaljit Singh explained nearly two decades ago, "[t]ransnational corporations are among the world's biggest economic institutions. A rough estimate suggests that the 300 largest TNCs own or control at least one-quarter of the entire world's productive assets, worth about US$5 trillion." Jed Greer & Kavaljit Singh, *A Brief History of Transnational Corporations*, GLOBAL POL'Y F. (2000), https://www.globalpolicy.org/empire/47068-a-brief-history-of-transnational-corporations.html.

110. Alexandre Faite, *Involvement of Private Contractors in Armed Conflict: Implications under International Humanitarian Law*, 4 DEF. STUD. 166, 1 (2004) (some companies "have carried out active combat operations in various countries").

111. *See* Kathy Gilsinan, *The Return of the Mercenary*, ATLANTIC (Mar. 25, 2015), https://www.theatlantic.com/international/archive/2015/03/return-of-the-mercenary/388616/ ("Before the Peace of Westphalia in 1648

governments in terms of the personnel they contribute, the buildings they protect, and the force they are authorized to use is blurring.

In @WAR, national security journalist Shane Harris provides several examples of how governments rely on companies to "design weapons, move and feed troops, [and] build and maintain aircraft, ships, and satellites."[112] The private sector contributes vital services to militaries, such as logistical and administrative support. Among the for-profit actors are military contractors who develop weapons systems and machinery,[113] private security firms that offer trained personnel and tactical support,[114] venture capitalist firms and tech incubators that support innovation in intelligence and military operations,[115] and the tech giants that host open platforms and hold a tremendous amount of the world's data.[116] In the past few decades, government monopolies on war have increasingly yielded space to the private market. As Singer expounds, "[f]rom companies like Blackwater doing armed convoy escort jobs in Iraq . . . and CACI interrogators working at Abu Ghraib, to the outsourcing of the U.S. military supply chain to firms like Halliburton . . . private companies are operating in traditional military roles as never before."[117] There is greater involvement and, as a result, influence by for-profit companies, incentivized by financial gain, in modern warfare. It is important to note that the use of private military contractors is not limited to powerful states like the United States,[118] but is becoming more common in the Global South as well. For ex-

---

ended Europe's Thirty Years' War and marked the rise of the modern state system, medieval powers from kings to popes routinely hired private fighters to do battle for them.").

112. HARRIS, *supra* note 5, at xxi.

113. Examples include Northrop Grumman, BAE Systems, Lockheed Martin.

114. Examples include CACI and Aegis Defence Services.

115. *See generally* John T. Reinert, *In-Q-Tel: The Central Intelligence Agency as Venture Capitalist*, 33 NW. J. INT'L L. & BUS. 677 (2013) (providing background on the example of In-Q-Tel).

116. Examples include Facebook, Twitter, Amazon, YouTube, and Google.

117. SINGER, *supra* note 10, at 370–71.

118. *See* HERBERT WULF, INTERNATIONALIZING AND PRIVATIZING WAR AND PEACE 169–94 (2005) (discussing the privatization of military services in the United States and the United Kingdom).

ample, in 2004, the Cote d'Ivoire government hired a private military firm from Israel to run its intelligence operations and private pilots from Belarus to provide air support against French troops.[119]

In addition to the emergence of private sector manpower, new technologies also disrupt the more traditional role of military contractors in designing and building weapons and military equipment. Military contractors hold a vast cache of government secrets, such as designs for fighter jets and weapons systems. While physical buildings are relatively easy to protect, military contractors can be infiltrated in the cyber dimension from a distance and without much expense. As Harris reveals, military contractors were slow to guard their cyber perimeters and, as a result, were targeted by foreign agents. In 2006, a number of military contractors in the United States were hacked.[120] The intruders stole a large amount of data, including schematics for a next-generation aircraft.[121] The development of this jet cost roughly $337 billion and development took place over many years, if not decades.[122] The operation, for which China's military was the primary suspect, marked one of the first major espionage thefts between governments without a corresponding physical intrusion.[123]

In response to newly recognized cyber threats, new private-public partnerships emerged between the U.S. government and Silicon Valley, which ironically distributes even more of the burden of protecting the nation's secrets and security among private actors.[124] While much of this alliance's operations are unknown to the public, insiders leaked infor-

119. Singer recounts how these mercenaries caught French troops off guard when they deployed to enforce a cease-fire with rebel groups: "On November 4, 2004, two Israeli-made Aerostar drones circled above their base, scouting out targets and establishing their GPS coordinates. A few hours later, Russian-made Sukhoi jet fighters screamed in, dropping bombs, which killed nine French soldiers and one U.S. aid worker." SINGER, *supra* note 10, at 268.

120. HARRIS, *supra* note 5, at x–xi.

121. *Id.* at x.

122. *Id.*

123. *Id.* at xi.

124. *Id.* at xx.

mation that provides insight into the extent of cooperation.[125] Journalists report that Google gave the Pentagon special access to its machine-learning software to help analyze images from drones, and that Amazon provided artificial intelligence software to the U.S. military.[126] Further, more and more vital infrastructure is privately owned, including "banks, power grids, shipping systems, hospitals and internet-linked security cameras, cars and appliances."[127] This creates confusion over which entity—government or private owner—is responsible for defending this infrastructure and who can respond to an attack.[128] In addition, social media platforms and other technology companies are acquiring vast amounts of data on private citizens, the breach of which could threaten national security, among other things.[129]

The past decade also witnessed a rise in a new type of mercenary: the cyber mercenary.[130] Private companies are responsible for supplying cyber weapons and digital surveillance tools to repressive regimes,[131] such as the government of Sudan,

125. For example, Edward Snowden famously leaked millions of documents revealing tech companies' cooperation with the NSA. *See generally* GLENN GREENWALD, NO PLACE TO HIDE (2014).

126. David Meyer, *Amazon and Google Are Cultivating Quiet Ties with Police and Military. That's Becoming a Big Problem*, FORTUNE (May 23, 2018), http://fortune.com/2018/05/23/amazon-aclu-police-google-military/.

127. Sanger, *supra* note 25.

128. *Id.* ("The range of American targets is so wide and deep that it's almost impossible to understand all of the vulnerabilities. And because most of those targets don't belong to the government . . . confusion reigns over who is responsible for defending them and who will decide when to strike back.").

129. In a recent incident, a private company called Strativa, which sells athletic trackers published GPS data from its customers which clearly highlighted the location of military bases. Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret U.S. Army Bases*, GUARDIAN (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

130. *See generally* TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER (Cambridge University Press 2018).

131. Alex Hern, *Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim*, GUARDIAN (July 6, 2015), https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

whose president is notably under ICC indictment.[132] Governments all over the world enlist the skills of hackers from private corporations and less formal organizations.[133] Through these connections, private companies not only provide military support on the physical battlefield, but in cyberspace. Engagement of a private entity in offensive cyber operations raises questions about the engaged party's authority to use force,[134] the state's responsibility for their acts, and how the other government may respond under international law. The use of non-state cyber operatives by countries like China, Russia, and Syria is also notably on the rise.[135] While in the past such hackers likely acted independently, there is ample evidence that many hackers today take orders from their governments.[136]

In addition, terrorist groups today show a proclivity towards using the internet and social media in creative and innovative ways. The decentralized nature of the internet allows these groups to broadcast their message around the world.[137] For example, al-Qaeda and ISIS both show a great deal of ingenuity in their use of technology—particularly to spread propaganda, radicalize, organize, plan, and recruit.[138] Al-Qaeda and ISIS use the internet to engage new members and multiply their numbers of both physical fighters and digital jihadists. Understanding the centrality of the exploitation of social media to ISIS's rise is necessary for understanding how the organ-

132. *Id.* (describing how leaked documents from an infamous cyber firm show sales of hacking tools to the Government of Sudan); Prosecutor v. Al Bashir, ICC–02/05–01/09, Warrant of Arrest, at 8 (Mar. 4, 2009).

133. Mark Mazzetti, Adam Goldman, Ronen Bergman & Nicole Perlroth, *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*, N.Y. TIMES (March 21. 2019), https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html.

134. Whether or not cyber-attacks qualify as force is a major debate and one that is not addressed here. *See, e.g.*, Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 458-459 (2011) (on the difficulty of legal line-drawing around cyber-attacks and differing perspectives between countries that will make "interpretive agreement" over Article 2(4) of the UN Charter applies to cyber-attacks).

135. MAURER, *supra* note 130, at 81–117 (describing cyber activities by Iran, Syria and countries of the former Soviet Union, and how targets such as the United States have responded).

136. *Id.*

137. *Id.* at 209.

138. In Iraq, al-Qaeda operatives downloaded images of U.S. military bases off of Google Earth. *Id.* at 207.

ization grew so quickly.[139] By first broadcasting their atrocities, such as beheadings, across the internet, ISIS created a reputation for being so brutal that many opted for flight over facing such a ruthless foe.[140] ISIS thereby seized major swaths of territory swiftly and without major resistance because their online-enhanced reputation preceded them. Even as ISIS loses some of this control over territory, the group's internet presence and online influence persists. To date, ISIS has produced thousands of videos and Twitter accounts.[141] The rise and fall of ISIS in Syria is a key example of how the informational dimension of warfare may begin before physical hostilities and continue long after the conclusion of battlefield operations.

The ongoing armed conflict in Syria serves as an informative example of cyber operations running in parallel to on the ground operations.[142] In 2011, a group of cyber operatives who conduct malicious online activities in support of the Bashir al Assad regime, known as the Syrian Electronic Army (SEA), emerged.[143] Despite their marketed image as an independent hacker collective, evidence shows that they are an organized group directly associated with Assad, as they grew out of the Syrian Computer Society, a group he once headed.[144]

---

139. *Id.* at 205–06.

140. *See generally* Simone Molin Friis, *'Beyod Anything We Have Ever Seen': Beheading Videos and the Visibility of Violence in the War Against ISIS*, 91 INT'L AFF. 725 (2015); James P. Farwell, *The Media Strategy of ISIS*, 56 GLOBAL POL. & STRATEGY 49 (2014); Imran Awan, *Cyber-Extremism: ISIS and the Power of Social Media*, 54 SOCIETY 138 (2017).

141. MAURER, *supra* note 130, at 240.

142. David E. Sanger & Eric Schmitt, *Hackers Use Old Lure on Web to Help Syrian Government*, N.Y. TIMES (Feb. 1, 2015), https://www.nytimes.com/2015/02/02/world/middleeast/hackers-use-old-web-lure-to-aid-assad.html ("The Syrian conflict has been marked by a very active, if only sporadically visible, cyberbattle that has engulfed all sides, one that is less dramatic than the barrel bombs, snipers and chemical weapons—but perhaps just as effective.").

143. Luke Harding & Charles Arthur, *Syrian Electronic Army: Assad's Cyber Warriors*, GUARDIAN (Apr. 30, 2013), https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background ("The Syrian Electronic Army (SEA) sprang up in 2011 at the beginning of the anti-Assad revolution.").

144. Stewart Kenton Bertram, '*Close enough*'*—The Link Between the Syrian Electronic Army and the Bashar al-Assad Regime, and Implications for the Future Development of Nation-State Cyber Counter-Insurgency Strategies*, 8 J. TERRORISM RES. 2, 6 (2017).

Ahmed K. Al-Rawi describes SEA as "cyber warriors who are closely connected to the Syrian government."[145] In addition to their activities within Syria, SEA is responsible for attacks in other parts of the world—for example, hacking into the Twitter feeds of influential institutions like the NEW YORK TIMES and WASHINGTON POST, and tweeting out pro-Assad commentary.[146] They have, however, gone further and engaged in activities that caused temporary, but significant, real-world damage. In 2013, SEA claimed credit for a hack of the Twitter account of the ASSOCIATED PRESS that tweeted that there was an explosion at the White House and that President Obama was injured.[147] This hack caused a significant crash in the stock market of about $136 billion.[148] As David Sanger details, SEA also stole critical documents from the Syrian opposition, which revealed tactical battle plans and data about the forces on the ground.[149] Both these attacks went beyond propaganda and caused measurable impacts in the real world.

In addition to formalized groups and informal networks of non-state actors involved in hostilities on the ground and in cyberspace, technology also empowers individuals. Lone wolf hackers and other malicious or profit-driven civilians, as well as benevolent citizens seeking to speak truth to power, use new technologies to contest government actions and confront the powerful with inconvenient truths. The internet has the transformative ability of bringing information to people's fingertips and amplifying the voices of individuals. It offers an unprecedented capacity for organizing the citizenry and has had a striking equalizing effect in allowing individuals and civilian groups to be louder, more influential, and ultimately more powerful on the global stage. As technology becomes more af-

145. Ahmed K. Al-Rawi, *Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army*, 40 PUB. REL. REV. 420, 420 (2014).

146. *Id.* at 423.

147. Max Fisher, *Syrian Hackers Claim AP Hack that Tipped Stock Market by $136 Billion. Is it Terrorism?*, WASH. POST (Apr. 23, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.ca0155df4778.

148. *Id.*

149. Sanger & Schmitt, *supra* note 142.

fordable, and as information becomes more open and fluid, individuals grow in power, capacity, and influence.[150]

In the cyber context, individuals may rival states and organizations in their ability to cause harm. For example, a lone wolf hacker developed the now-infamous Love Bug computer virus, which caused roughly $15 billion in damages.[151] Another example is a hacker referred to as *The Jester* who takes on governments and hacker groups, allegedly conducting over two hundred attacks.[152] Social media creates an end run around traditional authorities such as governments and media and enables connection among individuals across and around the world. While international law developed and granted international organizations and multinational corporations international legal personality, the framework has not yet adapted to address the empowerment and capabilities new technologies vest in individuals. These examples demonstrate the urgent need to investigate new challenges in applying the laws of war and, in particular, the principle of distinction.

B. *Taking Humans out of the Loop*

Technological advances in robotics, algorithmic programming, machine learning, and artificial intelligence (AI) led to a shift towards remote-controlled vehicles and autonomous systems in military operations. The twenty-first century has seen two especially interesting trends in unmanned vehicles. First, there is a growing diversification of unmanned vehicles—from self-driving cars and land roaming vehicles to unmanned maritime and submarine vessels to micro drones.[153] Second, there is a trend towards equipping such vehicles with software that

150. *See* SINGER, *supra* note 10, at 271 ("As a variety of scientists and analysts look at such new technologies as robotics, AI and nanotech, they are finding that massive power will no longer be held only by states. Nor will it even be limited to nonstate organizations like Hezbollah or al-Qaeda. It is also within the reach of individuals.").

151. JORDAN ET AL., *supra* note 1, at 69.

152. MAURER, *supra* note 130, at 17.

153. *See generally* Guowei Cai, Jorge Dias & Lakmal Seneviratne, *A Survey of Small-Scale Unmanned Aerial Vehicles: Recent Advances and Future Development Trends*, 2 UNMANNED SYSTEMS 175 (2014); KIMON P. VALAVANIS & GEORGE J. VACHSTEVANOS, HANDBOOK OF UNMANNED AERIAL VEHICLES (2014).

allows for their autonomous operation.[154] The autonomy of machines exists on a spectrum based on the degree of human involvement—from remote-controlled vehicles to autonomous vehicles that operate on a pre-planned narrative to vehicles that use machine learning so that UAVs can conduct tasks with limited or no human intervention.[155] This phenomenon raises unresolved significant legal questions about how to hold individuals accountable for harm caused by machines and computer programs based on machine learning and AI in autonomous systems. In addition, the use of drones and other remote-controlled vehicles also transform traditional hierarchies and command structures in the military, which will have major implications for the application of command responsibility in war crimes prosecutions.

While unmanned aerial vehicles, often referred to as UAVs or drones, have been used in military operations for decades—the Iraq and Afghanistan wars in the early twenty-first century marked a tipping point in their sophistication and prominence. As Singer describes, when U.S. forces went into Iraq, the original invasion had zero robotic systems on the ground. By the end of 2004, the number was up to 150. By the end of 2005, it was up to 2,400. By the end of 2006, it had reached the 5,000 mark and growing.[156]

In the military setting, UAVs and other machines or robots are increasingly used as replacements for soldiers physically on the ground. As Noel Sharkey explains, there has been an "exponential rise of the use of drones in the conflicts in Iraq and Afghanistan and by the US Central Intelligence Agency for targeted killings and signature strikes in countries outside the war zones: Pakistan, Yemen, Somalia, and the Philippines."[157] Unmanned vehicles refer to vehicles that can be operated remotely. While "[a]ttacking from a distance is noth-

154. Kristina Grifantini, *How to Make UAVs Fully Autonomous*, MIT TECH. REV. (July 15, 2009), https://www.technologyreview.com/s/414363/how-to-make-uavs-fully-autonomous/.

155. The recent evolution of AI is described in the story of AlphaGo, a computer created by a company called DeepMind to defeat a human Go world champion. *The Story of AlphaGo So Far*, ALPHAGO, https://deepmind.com/research/alphago/ (last visited Mar. 22, 2019).

156. SINGER, *supra* note 10, at 32.

157. Noel E. Sharkey, *The Evitability of Autonomous Robot Warfare*, 94 INT'L REV. RED CROSS 787, 788 (2012).

ing new," there are a number of newer technologies which enhance the ability to attack remotely.[158] It is not only the United States and other major powers that use UAVs for surveillance or targeted killings. As of 2011, over fifty States possessed military robotics capacity.[159] In addition, as the cost of drones decreases, they are increasingly available and popular among the civilian population as well, and it is not difficult to imagine how a commercial drone might be repurposed as a weapon with the appending of additional components.

More perplexing and perhaps more troubling is the use of autonomous systems in place of human decision makers. In more recent years, with the increase in computing power and advances in neural networks, computers are used to replace human cognition. Artificial General Intelligence (AGI), is merely one narrow category within the greater AI framework. AGI seeks to give computers general cognitive abilities, whereas the majority of AI specialties—machine learning, computer vision, and natural language processing, for example—focus on specific tasks.[160] Governments have already introduced AI programming in military operations to aid quick decision-making by enabling visualization and evaluation by a commander of his or her plans, as well as predicting the impact of a variety of effects.[161] For example, U.S. military intelligence officers use Real-Time Adversarial Intelligence and Decision-Making or RAID, an AI that scans a database of previous enemy actions within an area of operations to assist the commander with strategic decisions.[162]

C. *Information Warfare in the Digital Age*

While deception and the use of disinformation have long been tactics of successful war strategy, the capabilities and tools used to effectively disseminate disinformation have

158. William Boothby, *Some Legal Challenges Posed by Remote Attack*, 94 INT'L REV. RED CROSS 579, 579 (2012).

159. Noel Sharkey, *The Automation and Proliferation of Military Drones and the Protection of Civilians*, 3 LAW INNOVATION & TECH. 229, 239 (2011). ?

160. JASON: MITRE CORP., PERSPECTIVES ON RESEARCH IN ARTIFICIAL INTELLIGENCE AND ARTIFICIAL GENERAL INTELLIGENCE RELEVANT TO DOD 1 (2017), https://fas.org/irp/agency/dod/jason/ai-dod.pdf.

161. *See* SINGER, *supra* note 10, at 357 (describing DARPA's "Integrated Battle Command" system of AI aids).

162. *Id.*

evolved substantially. Conversations about fake news have permeated the public discourse in recent years with the emergence of evidence about how states and other political actors deploy, reshape, and target information for political gain, social manipulation, and criminality in the digital age.[163] In warfare, the spread of information and disinformation is multifaceted and powerful, and its dissemination is particularly significant in asymmetrical situations. While weapons cost money and military training requires the expenditure of time and resources, the strategic use of information is an effective method by which smaller, weaker, and poorer groups can outwit their more powerful foes.[164] Thus, increased awareness of the potential strategic uses of information provides a competitive advantage. Operationally, the ability of military commanders to effectively communicate orders to their troops and for disparate units to share accurate and timely intelligence is integral to success on the battlefield. Tactically, the internet provides an efficient means of spreading disinformation to confuse or deceive opposition forces. As Patrikarakos explains, "[f]or the first time in history, social networks and smartphone apps are being used as tools of war."[165] Social media empowers individuals and militaries, and is used as a tool by repressive governments and terrorist groups for spreading misleading or false information to unprecedented numbers of people.

The use of ICTs in warfare has a lengthy history. World War I was the first highly photographed war with journalists documenting the conflict and newspapers publishing images.[166] Radio and film played an integral role in World War II,[167] and news outlets of the day referred to the Vietnam

163. One catalyst for this debate was the 2016 U.S. presidential elections. *See generally* Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 J. ECON. PERSP. 211 (2017).

164. MARIA SNEGOVAYA, INST. FOR THE STUDY OF WAR, PUTIN'S INFORMATION WARFARE IN UKRAINE: SOVIET ORIGINS OF RUSSIAN'S HYBRID WARFARE 9 (2015).

165. PATRIKARAKOS, *supra* note 54, at 113.

166. Craig Allen, *Photographers on the Front Lines of the Great War*, N.Y. TIMES (June 30, 2014), https://lens.blogs.nytimes.com/2014/06/30/photos-world-war-i-images-museums-battle-great-war/.

167. *See* KEN SHORT, FILM AND RADIO PROPAGANDA IN WORLD WAR II (1983) (explanatory parenthetical).

War as the television war.[168] The Cold War provides a cogent example of just how crucial the strategic use of information can be in warfare and geopolitics.[169] Today, the current generation of ICTs is quickly turning conflicts in Syria and Iraq into the first social media wars, in which users generate photographs and videos of the war and post firsthand commentaries online, circumventing traditional media outlets and competing with state-sponsored narratives.[170]

The founding of YouTube in 2005 provided a mainstream outlet for distribution of user-created combat footage. By 2007, there were over seven thousand video clips of combat footage from Iraq on YouTube.[171] Drones and unmanned sensors captured some footage, which was then posted via official channels; anonymous or pseudonymous sources shared other videos shot with mobile phones.[172] With time, the trend of posting combat videos gained popularity and it currently plays a significant role in publicizing ongoing conflicts and creating potential evidence in Syria and Ukraine, for example.[173] While these videos can assist fact-finders, they may also make their work more difficult because of the massive volume of content and difficulty in its verification.

With so much available war footage, governments, terrorist groups, and other actors can mislead the public by re-using, repurposing, or mischaracterizing footage. For example, a video posted on Twitter showing the torture of detainees allegedly came from Syria, whereas on closer inspection, journalists found that it was more likely from Pakistan.[174] In addition, much of this footage is poor resolution, which makes it diffi-

168. George Bailey, *Television War: Trends in Network Coverage of Vietnam 1965–1970*, 20 J. Broadcasting & Electronic Media 147, 147 (1976).

169. *See* Linda Risso, Propaganda and Intelligence in the Cold War: The NATO Information Service (2014).

170. *See generally* P. W. Singer & Emerson T. Brooking, LikeWar: The Weaponization of Social Media (2018).

171. Singer, *supra* note 10, at 320.

172. *Id.*

173. *See* Patrikarakos, *supra* note 54, at 171 ("[D]uring times of crisis and war, content becomes data of a different kind. Every YouTube video posted from Ukraine or Syria becomes a possible piece of evidence about a suspected atrocity on the ground False").

174. Rao Komar, *How to Digitally Verify Combat Affiliation in Middle East Conflicts*, Bellingcat (July 9, 2018), https://www.bellingcat.com/resources/how-tos/2018/07/09/digitally-verify-middle-east-conflicts/.

cult to distinguish exactly what is happening and who is involved. Russian TV has shown real videos and satellite imagery but mischaracterizes what it actually depicts.[175] Russia has even tried to pass off screen captures from a video game as real combat footage allegedly portraying coordination between the United States and ISIS.[176] Snegovaya explains that social media contribute to "the spread of misleading and outright fake news that is able to reach wide audiences to a degree unprecedented in modern history."[177] These fake narratives have the concerning potential to influence conflict on the ground. Therefore, even if investigators identify the message as propaganda, the narratives cannot be ignored. Social media posts, true or not, are part of the story.

Social media platforms are the perfect propaganda tools for war.[178] Their usage for propaganda purposes appears in numerous conflicts. Militaries and anti-government groups alike use social media to recruit fighters and frame the conversation about their activities on the ground.[179] Governments invest significant resources in public diplomacy and soft power, which promote content that supports a government's version of events.[180] In the past, such narratives were hard to challenge, but competing narratives are gaining momentum with social media and smartphones. For example, when the Israeli army bombed a hospital and residential area in Gaza during the 2014 Operation Protective Edge, the Israel Defense Force Twitter account produced content alleging that Hamas used the hospital for planning attacks and storing weapons, and that they used human shields by hiding among the civilian population.[181] At the same time, Hamas ran a counter-campaign on social media claiming that Israel was targeting Palestinian civilians.[182] These competing narratives make it difficult

175. SNEGOVAYA, *supra* note 164, at 18.

176. Kyle Mizokami, *Russia Tried to Pass off a Video Game as Combat Footage*, POPULAR MECHANICS (Nov. 14, 2007), https://www.popularmechanics.com/military/a13612161/russia-tried-to-pass-off-a-video-game-as-combat-footage/.

177. PATRIKARAKOS, *supra* note 54, at 133.

178. SNEGOVAYA, *supra* note 164, at 31.

179. *Id.*

180. *See generally* Joseph S. Nye Jr., *Public Diplomacy and Soft Power*, 616 ANNALS AM. ACAD. POL. & SOC. SCI. 94 (2008).

181. PATRIKARAKOS, *supra* note 54, at 17–20.

182. *Id.*

for groups on all sides, and the outside world, to know whether or not the parties to the conflict are in compliance with international law.

Another compelling example is the Russian propaganda surrounding conflicts in Syria and Ukraine. The Russian government and military forces employ information deception practices from the Soviet era with a modern twist, taking advantage of all the new technologies available to them. National security analysts Max Bergmann and Carolyn Kenney have explained that while Russia's efforts are "rooted in old Soviet tactics, the new online information environment makes these current efforts a qualitatively different threat than those of the past."[183] The Russian military uses technology in a variety of ways: to conduct espionage, such as through hacking; to engage in information operations to disseminate disinformation, as well as spread and amplify information that advances a particular narrative; and to further propaganda campaigns using traditional and contemporary media platforms.[184]

Syria serves as a valuable example of how digital information warfare develops in practice and the consequences that it might have for those documenting the conflict, investigating potential crimes, and applying the law. The White Helmets are an organized group of volunteer rescue workers with a global media presence[185] who provide humanitarian aid to victims in Syria, document the government's war crimes, and spread information about what is happening on the ground to the world.[186] Since they are present in areas where journalists cannot go, they have become de facto journalists and media

183. *War by Other Means—How Russia's 'Active Measures' Weaponize Information*, DEMOCRACY DIG. (June 7, 2017), https://www.demdigest.org/war-means-russian-active-measures-weaponize-information/.

184. *See generally* SNEGOVAYA, *supra* note 164.

185. As Olivia Solon explains, "[t]he White Helmets, officially known as the Syria Civil Defence, is a humanitarian organization made up of 3,400 volunteers—former teachers, engineers, tailors and firefighters—who rush to pull people from the rubble when bombs rain down on Syrian civilians. They've been credited with saving thousands of civilians during the country's continuing civil war." Olivia Solon, *How Syria's White Helmets Became Victims of an Online Propaganda Machine*, GUARDIAN (Dec. 18, 2017), https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

186. WHITE HELMETS, https://www.whitehelmets.org/en (last visited Mar. 22, 2019).

sources. The White Helmets have a sophisticated website promoting their work and providing a platform through which outsiders can donate money in support of their efforts.[187] They maintain a Facebook page[188] and an active Twitter feed[189] to further propagate their message, and their work was the subject of a Netflix documentary that received an Academy Award. Furthermore, they have twice been nominated for the Nobel peace prize.[190] The documentary features footage taken by the group while conducting rescue efforts.[191]

Not only have the White Helmets accumulated significant documentary footage of the conflict, but they use social media to broadcast it to those outside Syria. Unlike more traditional humanitarian aid groups like the International Committee for the Red Cross (ICRC),[192] the White Helmets make no attempts to maintain neutrality. Instead, they play an important role in documenting the conflict and collecting evidence against the Assad Regime. In addition to its use in advocacy efforts, such documentation could also be used to establish legal accountability. For example, Solon explains that White Helmets' footage has been used to document the chemical attacks in Khan Sheikhoun and other parts of Syria.[193]

Their effective use of social media also made the White Helmets a target of an extraordinary disinformation campaign that positioned the group as terrorists with links to al-Qaeda.[194] According to journalist Emma Grey Ellis, the origin of this online campaign is traceable to the Russians: the "cam-

187. *Id.*

188. Syria Civil Defense, FACEBOOK, https://www.facebook.com/SyriaCivilDefence (last visited Mar. 22, 2019).

189. The White Helmets (@SyriaCivilDef), TWITTER, https://twitter.com/SyriaCivilDef (last visited Mar. 22, 2019).

190. Solon, *supra* note 185.

191. Maanvi Singh, *Young Syrian with a Dream Risks His Life to Film New Netflix Doc*, NPR (Sept. 26, 2016), https://www.npr.org/sections/goatsandsoda/2016/09/26/495005538/young-syrian-with-a-dream-risks-his-life-to-film-new-netflix-doc.

192. *See* Denise Plattner, *ICRC Neutrality and Neutrality in Humanitarian Assistance*, INT'L COMMITTEE RED CROSS (Apr. 30, 1996), https://www.icrc.org/en/doc/resources/documents/article/other/57jn2z.htm (describing what it means for the ICRC to be a "humanitarian, neutral, impartial and independent body").

193. Solon, *supra* note 185.

194. *Id.*

paign to discredit the White Helmets started at the same time as Russia staged a military intervention in Syria in September 2015."[195] This propaganda is spread across social media and on television news, creating a trail that, as Bellingcat demonstrates, can be traced back to the Russian government.[196] Even more mainstream avenues picked up this messaging. For example, in a speech to the United Nations, Canadian blogger Eva Bartlett[197] claimed that the White Helmets staged rescues and recycled victims—a claim that has since been thoroughly debunked.[198] Despite journalists exposing disinformation about the White Helmets, this misinformation tactic nevertheless successfully shaped the online conversation about the group.[199] By using bots, automation, and algorithms, the Russians flood content and create what Scott Lucas refers to as a "manufactured consensus."[200] These conflicting narratives create significant confusion around the activities and status of the White Helmets.[201] While the main goal of this false narrative may be simply to discredit the White Helmets, it is dangerously muddling the perception of their role in the conflict, making them out to be unlawful combatants who could be legally targeted by military efforts.

---

195. *Id.*

196. Bellingcat Investigation Team, *Chemical Weapons and Absurdity: The Disinformation Campaign Against the White Helmets*, BELLINGCAT (Dec. 18, 2018), https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons-and-absurdity-the-disinformation-campaign-against-the-white-helmets/.

197. Eva Bartlett is a Canadian blogger who covers the Syrian conflict and frequently appears on Russian TV. Eva Bartlett, *About Me*, IN GAZA & BEYOND, https://ingaza.wordpress.com/about-me/ (last visited Mar. 24, 2019). Many of her public assertions have been demonstrated to be false, and some would characterize them as conspiracy theories and misinformation. Solon, *supra* note 185.

198. Patrick Worrall, *Eva Bartlett's Claims About Syrian Children*, CHANNEL 4 NEWS (Dec. 20, 2016), https://www.channel4.com/news/factcheck/factcheck-eva-bartletts-claims-about-syrian-children.

199. *See generally* Solon, *supra* note 185.

200. Scott Lucas, *Who are Syria's White Helmets, and Why are They so Controversial?*, CONVERSATION (Oct. 7, 2016, 8:48 AM), http://theconversation.com/who-are-syrias-white-helmets-and-why-are-they-so-controversial-66580.

201. *See* SYRIA CAMPAIGN, KILLING THE TRUTH: HOW RUSSIA IS FUELLING A DISINFORMATION CAMPAIGN TO COVER UP WAR CRIMES IN SYRIA 3 (2017) ("[T]he vicious smearing of the White Helmets, especially false terrorism claims, are designed to undermine the evidence they collect and legitimise their killing.").

The weaponization of social media and the mass dissemination of disinformation is not unique to the Syrian context. In Ukraine, Russia uses similar tactics to confuse the world and their opponents about their activities and goals in occupying Crimea.[202] In a very different context, journalists allege that extremist monks in Myanmar used Facebook to spread hate speech against the Rohingya population, possibly contributing to an escalation in violent attacks.[203] Allegations of fake news to discredit facts, alongside the free flow of actual fake news, leads to a disturbing trend in delegitimizing important institutions. Given this growing complexity, it is more essential than ever before that judges uphold high standards when vetting information in criminal cases. Rigorous vetting will help any judge not only avoid contributing to misinformation and being discredited, but also yield better decisions and support the rule of law around the world.

IV. Law in Conflict

The laws of war reflect the geopolitics of the time in which they were created and expose inherent assumptions about the society and culture. For example, the laws of war were originally predicated on conflict between states,[204] and later expanded to include civil war between states and internal organized armed groups.[205] However, with the changing nature of war and society brought about by technological innovation, many of the traditional assumptions are now irrelevant or invalid. There are a growing number of factual scenarios for which existing laws do not clearly and easily apply. As technology changes power dynamics between belligerents and blurs the line between civilians and combatants, many of the tradi-

202. Snegovaya, *supra* note 164, at 11–12.

203. Megan Specia & Paul Mozur, *A War of Words Puts Facebook at the Center of Myanmar's Rohingya Crisis*, N.Y. Times (Oct. 27, 2017), https://www.nytimes.com/2017/10/27/world/asia/myanmar-government-facebook-rohingya.html; Steve Stecklow, *Why Facebook is Losing the War on Hate Speech in Myanmar*, Reuters, Aug. 15, 2018, https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

204. *War and International Humanitarian Law*, Int'l Committee Red Cross (Oct. 29, 2010), https://www.icrc.org/en/doc/war-and-law/overview-war-and-law.htm ("International humanitarian law is part of the body of international law that governs relations between States.")

205. Ryngaert, *supra* note 55.

tional legal classifications stemming from the Hague[206] and Geneva Conventions[207] no longer fit. In addition, technologies that supplant physical and cognitive human functions in military operations raise significant legal questions about how to determine an individual's liability for certain harms.

Before the establishment of international criminal tribunals, national military courts served as the primary mechanism for holding individuals accountable for violations of IHL. The establishment of the International Criminal Tribunals for the former Yugoslavia and Rwanda (ICTY and ICTR, respectively) created a new pathway for enforcing IHL against individuals at the international level and generated a new source of law—case law—which enabled evolution of statutory rules through judicial interpretation. While the jurisprudence of the ICTY, ICTR, and now the ICC, assist in keeping the application of the law current with changing times, an assessment of whether certain laws are so obsolete that they cannot be reasonably interpreted to address present-day factual scenarios is nevertheless worthwhile. The following sections examine the adequacy of existing substantive laws for addressing modern warfare, taking into account the role played by new actors, as well as the changing roles of more traditional actors caused by the introduction of new technologies.

A. *The Principle of Indistinction*

The laws of war, or IHL, is traceable back to Hugo Grotius' 1625 Treatise ON THE LAW OF WAR AND PEACE.[208] Since then, IHL has evolved with several significant developments occurring in the twentieth century, including the Hague Convention in 1907, the Geneva Conventions in 1949, and the Additional Protocols in 1977. These substantive treaties were drafted, for the most part, in response to major wars between nation-states. Thus, the principles developed for IHL are typically reactive.[209] In the post-1945 period, there were additional

206. Law and Customs of War on Land (Hague, IV) art. 3, Oct. 18, 1907, 36 Stat. 2277, T.S. No. 539.

207. Fourth Geneva Convention, *supra* note 32, art. 4.

208. *See generally* HUGO GROTIUS, ON THE LAW OF WAR AND PEACE (A.C. Campbell, A.M. ed. & trans., Batoche Books 2001) (1625).

209. As Michael Schmitt and Sean Watts explain, IHL is a highly reactive body of law that has seen evolutionary and even revolutionary changes instituted by States following armed conflicts—the classic example being adop-

advances regarding the restricted use or prohibition on certain types of weapons. For example, the Biological Weapons Convention in 1972[210] and the Chemical Weapons Convention in 1993,[211] which strengthened the 1925 Geneva Protocol by "extending prohibitions to the development, production, acquisition, stockpiling, retention and transfer of biological and chemical weapons, and requiring their destruction."[212] However, despite a spate of wars and a series of protracted internal armed conflicts in the twenty-first century, there have been very few concrete IHL developments since the turn of the millennium.

In IHL, the rules that govern armed conflicts fall into two categories: (1) *jus ad bellum*, which governs the initiation of war, and (2) *jus in bello*, which governs the conduct of the warring parties.[213] *Jus in bello* has multiple sources of law, including treaties that govern the conduct of hostilities, conventions that limit the use of specific weapons, and principles of customary law—such as the principles of proportionality, distinction, and military necessity.[214] En masse, weapons ban treaties and the rules restricting weapons usage remain effective today. The implementation and enforcement of weapons bans is dif-

---

tion of the four Geneva Conventions in the aftermath of the Second World War. Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 TEX. INT'L L.J. 189, 191 (2015) (characterizing IHL as a "highly reactive body of law").

210. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, *opened for signature* Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

211. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, *opened for signature* Sept. 3, 1992, 1975 U.N.T.S. 45.

212. *Weapons*, INT'L COMMITTEE RED CROSS (Nov. 30, 2011), https://www.icrc.org/en/document/weapons; *see also* Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, 1342 U.N.T.S. 137, *as amended* Dec. 21, 2001, 2260 U.N.T.S. 82; Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, Sept. 18, 1997, 2056 U.N.T.S. 211.

213. FRITS KALSHOVEN & LIESBETH ZEGVELD, CONSTRAINTS ON THE WAGING OF WAR: AN INTRODUCTION TO INTERNATIONAL HUMANITARIAN LAW 1 (4th ed. 2011).

214. *Id.* at 3–5.

ficult, but the laws themselves are still applicable in the current contexts. The more challenging application of IHL in contemporary armed conflicts, and the focus of this section, centers around the rules and principles designed to protect civilians.

The principle of distinction dictates that, "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants."[215] Thus, the principle of distinction obliges that the parties to an armed conflict distinguish between the civilian population and combatants at all times.

> [T]his clear division between civilians and combatants is only about two centuries old, despite the uncounted millennia of warfare. It is a product of the Western organisation of war appearing with the standing armies, consolidating with the decline of other forms of armament in the face of a trained, uniformed, paid military.[216]

As previously discussed, the rise of non-state armed groups, the increased participation of corporate personnel in military operations, and the overall lack of distinction between actors on the modern battlefield complicate the application of this fundamental rule. In particular, the blurring line between combatants and civilians caused by the increased use of private actors and other irregular forces makes the applicability of the principle of distinction increasingly difficult.

In modern conflicts, terrorists and insurgents blend with the civilian population, and civilian actors are increasingly involved in military operations. For example, civilian engineers may be on the battlefield repairing drones while the pilots who operate the drones are thousands of miles away. With the increased involvement of a diverse variety of non-state actors including corporate mercenaries, cyber proxies, and increasingly engaged civilians inserting themselves into ongoing hostilities, it may no longer be a reasonable expectation for parties to draw such clear distinctions in the midst of the fog

215. Protocol I, *supra* note 32, art. 48.

216. Gunner Lind, *Modern Conflict Blurs the Line Between Soldiers and Civilians*, CONVERSATION (July 16, 2014), http://theconversation.com/modern-conflict-blurs-the-line-between-soldiers-and-civilians-28929.

of war. When civilian contractors wear clothing identical to military personnel and insurgents do all they can to blend in with the civilian population,[217] it becomes nearly impossible to differentiate among groups.[218] Corporate or surrogate warriors are neither civilians, "as they are not formally part of the military and its command structure," nor typical noncombatants, "as they are carrying out fundamentally military missions."[219] Whether certain military contractors, such as those repairing drones in the field or guarding black sites, are legally considered civilians—and therefore protected from enemy attack—requires a fact specific analysis.[220] Requiring such a complicated legal analysis is not necessarily a realistic expectation to place on military personnel in battlefield conditions.

This query is not theoretical—in fact, the issue is raised in a filing before the ICC Pre-Trial Chamber in which the Prosecutor requests to open an investigation in Afghanistan.[221] The filing states that "the nature of the crimes allegedly committed presented a number of challenges . . . caused by the multiplicity of anti-government armed groups operating in Afghanistan."[222] The filing also cites the Prosecution's inability to clearly "distinguish between diverse military actors or insurgents."[223]

On top of these complications created by the multitude of non-traditional actors engaged in military operations on the physical battlefield, the rise in cyber hostilities makes this assessment more complex than ever. Today, legal practitioners and academics still dispute what might qualify as cyber warfare versus cyberattacks that do not reach the armed conflict threshold. Although Additional Protocol I widened the field of

---

217. *See* SINGER, *supra* note 10, at 223 (describing the problem created when insurgents try to pass as civilians).

218. *Id.* at 221 ("Insurgents don't just take advantage of complex terrain (hiding out in the jungle or cities), they also do their best to mix in with the civilian population. They make it difficult for the force fighting them to figure out where they are and who they are.").

219. *Id.* at 372.

220. *See id.* (discussing factors bearing on the analysis of the legal status of military contractors).

221. Situation in the Islamic Republic of Afghanistan, ICC–02/17–7–Conf–Exp, Request for Authorisation of an Investigation Pursuant to Article 15, ¶ 30 (Nov. 20, 2017).

222. *Id.*

223. *Id.*

application of the law of armed conflict to encompass conflicts between government forces and some non-governmental groups, the law is nevertheless overly simplistic in light of the fluidity and multiplicity of armed groups in conflicts today.[224]

A confounding challenge to the application of IHL is that, unlike other areas of law which apply at all times, IHL has limited applications to situations of armed conflict.[225] This means that there is always a threshold consideration as to whether an armed conflict exists. The applicable legal provisions depend on whether there is an international or non-international armed conflict. As Sylvain Vité explains, "[d]epending on how the situations are legally defined, the rules that apply vary from one case to the next."[226] Some states characterized conflicts in Iraq, Syria, Libya, and Yemen as international and non-international at different times,[227] often changing the characterization as a means of justifying military actions on their part.[228] States can employ this subterfuge because, as Andreas Paulus and Mindia Vashakmadze discuss, such conflicts do not "clearly fit into the traditional pattern of either inter-state or internal conflict."[229]

---

224. *Cf. id.* ¶ 73 (listing the numerous and diverse contextual elements of a crime against humanity).

225. *What Is International Humanitarian Law?* INT'L COMMITTEE RED CROSS (JULY 2004), https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf ("International humanitarian law applies only to armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence.").

226. Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INT'L REV. RED CROSS 69, 70 (2009).

227. ARIMATSU & CHOUDHURY, *supra* note 65, at 42 (describing the challenge of applying classifications to the complex facts of these three conflicts and concluding that more research is necessary).

228. *See* Andreas Paulus & Mindia Vashakmadze, *Asymmetrical War and the Notion of Armed Conflict—A Tentative Conceptualization*, 91 INT'L REV. RED CROSS 95, 115 (2009) ("[M]any states, while launching military operations against [terror] groups and organizations, are not ready to accept the existence of armed conflict within their boundaries. If they admit that there is an armed conflict, they tend to argue that the so-called war on terrorism constitutes a new type of armed conflict to which international humanitarian law does not apply.").

229. *Id.* at 111.

B. *Accountability in the Age of Intelligent Machines*

In 2012, IHL expert William Boothy suggested that autonomous decision-making by machines and the corresponding issues which arise in regard to liability for such programs was, at that time, "grounded in fiction."[230] In his view, the issue was not ripe for debate as the technology was not yet able to take over human decision-making.[231] He did, however, note that "as technology becomes more complex and as decision-making relies increasingly on AI and less and less on human perception and judgment, the focus for responsibility may be expected to shift from planners and commanders to software engineers and the robots they beget."[232] It is debatable whether Boothy was correct about the elementary stage of this technology in 2012, but in 2019 it is quite clear that machine learning and other forms of artificial intelligence are more advanced and increasingly used by militaries.[233] Nevertheless, scholars and lawmakers still have not had the necessary legal debate. It is apparent that technology has reached a point at which it is no longer a matter of *whether* AGI will happen, but *when* it will happen. Lawyers, therefore, should consider the scenarios posed by Isaac Asimov and other science fiction writers, and discuss how establishing criminal liability and particularly criminal intent might differ in this new environment.

Autonomous systems may be a great asset to those on the battlefield, but they unquestionably complicate the laws of war and the process of establishing responsibility. IHL is tied to state responsibility, whereas the underlying principles of ICL are grounded in individual criminal responsibility. Individual criminal responsibility requires not only evidence that the law was violated, but also requires proof of specific and contextual elements of a clearly-defined crime beyond reasonable doubt.[234] It also requires that the accused individual can be

230. Boothby, *supra* note 158, at 595.

231. *Id.*

232. *Id.*

233. *See generally* M. L. Cummings, Chatham House, Artificial Intelligence and the Future of War (2017); Tejaswi Singh & Amit Gulhane, *8 Key Military Applications of Artificial Intelligence in 2018*, Market Research Blog (Oct. 3, 2018), https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018.

234. International Criminal Court (ICC), *Elements of Crimes*, 2011, ISBN No. 92-9227-232-2, available at: https://www.refworld.org/docid/

linked to the crime, sometimes with a requisite level of intent to establish liability.[235] These methodologies must be reconsidered if IHL and ICL are to keep up with the growing use of autonomous systems and AI. The question remains as to who is responsible when drones, robots, or other machinery with varying degrees of automation are used to attack civilians or violate the laws of war. This article does not attempt to answer this complex question, for which more research and debate is clearly necessary, but rather emphatically urges that international criminal law practitioners engage in these debates immediately. The conversation cannot wait.

C. *Remote Commanders and Command Responsibility*

Digital ICTs and robotics technologies not only disrupt traditional military operations and the composition of the battlefield, but also displace the traditional military structures of command and control. In recent years, the introduction of new technologies has led state militaries to move away from traditional hierarchies towards a flatter or networked command structure.[236] In fact, with every new advancement in communications technologies, "connections between the soldiers in the field and those commanders giving them battle orders [are] distanced," and, as a result, may be distorted.[237] When military commanders are on the ground, leading their troops on the battlefield, it is fairly easy to show their authority over their subordinates. However, if military commanders give orders from a distance and are more attenuated from their ground troops, it is more difficult to prove their authority, control, and knowledge of any criminal acts committed by those on the battlefield.

Military commanders and other superiors may be criminally responsible for war crimes committed by their subordinates if they knew, or had reason to know, that the forces

4ff5dd7d2.html [accessed 4 April 2019] (This ICC founding document lays out elements—both actus reas and mens rea—that must be proved for each crime codified in the Rome Statute).

235. *Id.*

236. As Singer explains, the "traditional concept of a military operation is a pyramid, with the strategic commander on top, the operational commanders next, and the tactical commanders on the bottom layer." SINGER, *supra* note 10, at 352.

237. *Id.* at 348.

under their control were about to commit or were committing such crimes and did not take all necessary and reasonable measures in their power to prevent their commission.[238] Thus, Article 28 of the Rome Statute requires the commander have effective control before the court will impose command responsibility for war crimes carried out by subordinates.

In 2016, Jean-Pierre Bemba Gombo was the first defendant at the ICC convicted of war crimes and crimes against humanity under the theory of command responsibility.[239] Eighteen months later the Court overturned his conviction on appeal.[240] The grounds for appeal were tied to the application and proof of command responsibility, leaving uncertainties about this mode of liability and how it must be proved in court. Two of the judges who joined the Appeals Chamber's majority opinion conceded in a separate writing that command responsibility is not a one-size-fits-all offense.[241] While that sort of flexibility is necessary and positive, some of the other assumptions made by the judges do not account for practical realities in the field. For example, the judges assert that what is required of a commander "depends on how proximate they are to the physical perpetrators in the chain of command."[242] In other parts of the decision they reference the fact that Bemba was based in the DRC while his troops committed their crimes in CAR, and that the great physical distance between them made it impossible for him to control so many troops effectively.[243] Instead, the judges suggested, such con-

238. Rome Statute, *supra* note 33, art. 28; *see also*, *Rule 153. Command Responsibility for Failure to Prevent, Repress or Report War Crimes*, INT'L COMMITTEE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule153 (discussing the facets of this rule within the context of IHL) (last visited Mar. 24, 2019).

239. Prosecutor v. Bemba, ICC–01/05–01/08, Judgment, ¶ 742 (Mar. 21, 2016) [hereinafter Bemba Trial Judgment].

240. Prosecutor v. Bemba, ICC–01/05–01/08 A, Judgment, ¶ 197 (June 8, 2018) [hereinafter Bemba Appeal Judgment].

241. Prosecutor v. Bemba, ICC–01/05–01/08–3636–Anx2, Separate Opinion of Judge Christine Van den Wyngaert & Judge Howard Morrison, ¶ 33 (June 8, 2018) [hereinafter Bemba Appeal Separate Opinion].

242. *Id.*

243. INTERNATIONAL CRIMINAL COURT, SUMMARY OF THE APPEAL JUDGMENT IN THE CASE *The Prosecutor v. Jean-Pierre Bemba Gombo* ¶ 25, https://www.icc-cpi.int/itemsDocuments/180608-bemba-judgment-summary.pdf.

trol lies with those who work more closely with the soldiers in the field.[244]

However, the judges seem to overlook some of the modern communications technologies which could have been, and likely were, used by Bemba to communicate with and control the actions of his troops on the ground—including the sophisticated Thuraya Satellite phones referred to in the evidence.[245] Using Thuraya phones, Bemba could have transmitted orders in real time to even the lowest-level troops in the field.[246] Such satellites can also be used to transmit live video, permitting commanders to see action on the ground in real time.[247] Singer points out that "generals at a distance are now using information technology to interpose themselves into matters that used to be handled by those on the scene and at ranks far below them."[248] As a result, generals halfway around the world can nevertheless be involved in detailed battle decisions as they occur.[249]

Thus, new technologies link commanders to the battlefield from great distances, effectively ending the separation of time and distance. Interestingly, studies of militaries using these technologies show a trend towards centralization of command and micromanagement, as well as the flattening of command chains, resulting in confusion of traditional communication channels.[250] For example, during U.S. combat missions in Iraq and Afghanistan, drone pilots based in Nevada complained that it was sometimes unclear under which chain of command they fell.[251] Further, those sitting behind a screen, so-called "tactical generals," often "overestimate how much they really know about what is happening on the ground."[252] Technology also enables more commanders to watch a battle

244. Bemba Appeal Judgment, ICC–01/05–01/08 A, ¶¶ 167, 171.

245. Bemba Trial Judgment, ICC–01/05–01/08, Judgment, ¶ 396 (Mar. 21, 2016).

246. *Cf.* SINGER, *supra* note 10, at 349 (describing the capacity as of 2009 for generals to send real-time instructions to captains in the field, utilizing radio communication and Predator video technology).

247. *Id.*

248. *Id.*

249. *Id.* at 350.

250. *Id.* at 353.

251. *Id.* at 386.

252. *Id.* at 350.

play out live from anywhere in the world. For example, in Afghanistan, numerous officers and commanders watched and weighed in to a broadcast of a drone video of battle in the Shah-i-Khot Valley sent to U.S. military bases around the world.[253] One problem with this new dynamic of supervision and command is that courts and investigators may interpose assumptions on what commanders see and neglect to consider what might not be visible in the footage.[254]

Given the rate of technological advancement, future ICC cases will require current military experts be up to date with technology. Such experts must have specific knowledge regarding cyber operations and the use of remote and autonomous systems so that judges have sufficient background information regarding the use of technology in communicating orders before the court issues a judgment. This technical knowledge is an essential prerequisite for understanding how to weigh certain types of evidence, particularly linkage evidence.[255] Additionally, it will be especially important that assumptions are not made about conflicts in developing countries, where the court may be inclined to underestimate their technological capacity if not properly educated. As the previous sections demonstrate, technology is the great equalizer. Old assumptions about the capacity, military strength, and political power of individuals and non-state groups may no longer hold true.

V. Truth in Conflict

In a 1918 speech following World War I, U.S. Senator Hiram Johnson stated, "[t]he first casualty when war comes is

253. *Id.* at 352.

254. *See id.* at 351 (discussing the range of misperceptions that can result when watching a conflict from afar).

255. As WITNESS' Video as Evidence Field Guide explains: "Linkage evidence is relevant and reliable information that helps prove responsibility for the crime. In other words, it helps prove who committed the crime and how they did it (e.g. individual perpetration, conspiracy, aiding and abetting, or command responsibility). This could include footage of military vehicles, uniforms, patches on uniforms, weapons, military offices, perpetrators training their forces, speeches where the suspect admits she or he was in command of the forces who perpetrated the crime, etc." WITNESS, Video as Evidence: All About Evidence 42 (2016), https://vae.witness.org/video-as-evidence-field-guide/.

truth."[256] The thought might not have originated from the senator, however. Some ascribe the adage to the Greek philosopher Aeschylus in about 500 BC.[257] Around that same period, Sun Tzu expressed a similar sentiment, that "[a]ll warfare is based on deception."[258] Clearly, in warfare, the strategic use of information, and especially disinformation, is nothing new. However, with the evolution of the internet, the development of interactive web-based platforms, and the proliferation of smartphones, the universe of available information is leading to a more complex and broader environment for waging information warfare. The complexity continues growing, with increasing connectedness and faster speeds of information transmission. Starting from Senator Johnson's premise, this section examines whether the truth can be resurrected after the fact and in the courtroom.

The obscuring of objective fact in times of war presents difficult operational challenges to criminal investigators, whose mandate obliges that they establish the truth.[259] Accurate fact-finding is an essential prerequisite for ensuring successful criminal prosecutions and fair trials, but one that is far from easy in the international context and particularly in investigations at the ICC.[260] Digital technologies such as smartphones and social media create novel challenges and unprecedented opportunities for international criminal investigators. For example, advances in technology and science can

256. *See* RESPECTFULLY QUOTED: A DICTIONARY OF QUOTATIONS REQUESTED FROM THE CONGRESSIONAL RESEARCH SERVICE 360 (Suzy Platt ed., 1989).

257. Brian W. Bowen & Stephen A. Karl, *In War, Truth is the First Casualty*, 13 CONSERVATION BIOLOGY 1013, 1013 (1999).

258. SUN TZU, *supra* note 27, at 66.

259. The Rome Statute instructs that the Prosecutor shall, "[i]n order to establish the truth, extend the investigation to cover all facts and evidence relevant to an assessment of whether there is criminal responsibility under this Statute, and, in doing so, investigate incriminating and exonerating circumstances equally . . . ." Rome Statute, *supra* note 33, art. 54.1(a).

260. There have been several cases at the ICC which have failed to meet the requisite evidentiary burden. *See* Patryk Labuda, *The ICC's 'Evidence Problem*,' VOLKERRECHTSBLOG (Jan. 18, 2019), https://voelkerrechtsblog.org/the-iccs-evidence-problem/ ("[T]he Prosecutor has on several occasions failed to clear Article 61's lower evidentiary threshold of 'substantial grounds to believe' that a suspect is responsible for the crimes he or she is charged with.").

aid in the documentation and reconstruction of attacks,[261] the identification of witnesses and other leads,[262] and the collection and analysis of evidence.[263] Moreover, as criminal activity increasingly involves digital devices and utilizes the internet, cyber investigations and digital investigative analysis may provide a strong evidentiary foundation for war crimes cases before international and national courts. At the same time, the ephemeral nature of digital information, the ease with which it can be distorted, and the effectiveness of encryption seriously thwart the fact-finding process.

Today, a vast amount of information with potential evidentiary value exists, in whole or in part, in digital format. This includes public statements, user-generated content,[264] social media evidence, and other open source information disseminated through the internet. It also includes private or closed-source material such as emails, text messages, digital audio or visual files, and documents—all of which may be created, transmitted, or stored on personal electronic devices. This section explores how the use of technology in armed conflicts presents obstacles for international criminal investigators and others engaged in the fact-finding process, while simultaneously offering cutting-edge investigative and analytical opportunities that capitalize on new innovations in the pursuit of truth, justice, and accountability. Through analyzing the transforming information environment in twenty-first century warfare and war crimes investigations, this section underscores the importance of strong evidentiary rules and clear procedural guidelines and brings attention to several deficiencies in the existing framework.

---

261. For example, digital architecture firm SITU Research explains how they used computer software to reconstruct crime scenes in Timbuktu, Mali. *ICC Digital Platform: Timbuktu, Mali*, SITU RES., https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali (last visited March 24, 2019).

262. WITNESS, *supra* note 255, at 112 (discussing how camera footage can be used to help link perpetrators to crimes).

263. *See* VERIFICATION HANDBOOK: AN ULTIMATE GUIDELINE ON DIGITAL AGE SOURCING FOR EMERGENCY COVERAGE (Craig Silverman ed., 2016), http://verificationhandbook.com/downloads/verification.handbook.pdf (discussing how technologies such as social media can be used to build bodies of evidence).

264. *See* Rebecca J. Hamilton, *User-Generated Evidence*, 57 COLUM. J. TRANSNAT'L L. 1, 3–4 (2018) (discussing the prospects for user-generated content to be used as evidence in international criminal cases).

A. *The Digitalization of Evidence*

Based on the evolving strategic use of information in the modern context, considering the sufficiency of the ICC's evidentiary rules and practice for addressing obstacles associated with the growing digital information environment is important. In order for the ICC to maintain credibility, it must ensure that evidentiary standards are sufficient to combat disinformation and identify truth. Traditionally, international criminal tribunals have been highly permissive with their evidentiary standards, leaving the judges with substantial discretion.[265] The ICC, like many other existing international tribunals, is based on a hybrid approach to procedure and evidence, borrowing elements from common law and civil law systems.[266] The relatively lax evidentiary standards in international criminal procedure draw from civil law systems, where an investigative judge often collects evidence, rather than the parties.[267] While this system functions well at the national level, there are apparent difficulties with its scalability to cases before the ICC. When trials last years and the body of evidence includes the testimony of hundreds of witnesses and thousands of documents, as is often the case at the ICC, the accompanying lack of rigor leads to a cluttered and confusing evidentiary record.[268] Even predating the influx of digital evidence, ICC investigations and cases have struggled to properly establish the facts to the requisite burden of proof.[269]

---

265. *See* Rome Statute, *supra* note 33, art. 69(4) ("The Court may rule on the relevance or admissibility of any evidence, taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness, in accordance with the Rules of Procedure and Evidence.").

266. JOHN D. JACKSON & SARAH J. SUMMERS, THE INTERNATIONALISATION OF CRIMINAL EVIDENCE 110–111 (2012).

267. *Id.* at 57–58. *See also* Patricia M. Wald, *The International Criminal Tribunal for the Former Yugoslavia Comes of Age: Some Observations on Day-to-Day Dilemmas of an International Court*, 5 WASH. U. J.L. & POL'Y 87, 90 (2001).

268. For a discussion of these problems by an ICC Judge see Prosecutor v. Gbagbo, ICC–02/11–01/15–1172–Anx, Dissenting Opinion of Judge Geoffrey Henderson, ¶¶ 3–4 (June 1, 2018).

269. In the Court's short history and with its small docket, there have been four denials to confirm charges in *Mbarushimana*, *Abu Garda*, *Kosey*, and *Ali*; one deferral of confirmation in *Gbagbo*; two full acquittals in *Ngudjolo* and *Bemba* and a partial acquittal in *Katanga*; a finding of no case to answer in

The introduction of digital evidence exacerbates these existing problems. A conviction based on a video that later proves to be fake or misleading would severely damage the credibility of the Prosecutor and the Court as a whole. As Patrikarakos points out, "[p]eople on the ground tweeting photos and descriptions of events during wartime have become invaluable—especially as they often tweet or post from areas too dangerous for journalists to go."[270] However, complication arises when veracity is inferred from volume despite the multitude of tools now available to buoy and disaggregate the distribution of misinformation. Disinformation derives from numerous sources on the internet, and false information may be spread by well-meaning individuals who believe it to be true. Therefore, certain traditional assumptions about the verification of information through corroboration do not necessarily translate in this new environment.

It is for this reason that tracing a video or image's first appearance online, tracking down the provenance, and identifying the original source are useful steps for proper source evaluation. International criminal investigators should learn how to exploit digital information effectively, authenticate it, and verify its contents to a standard sufficiently reliable in legal proceedings. Even more importantly, international judges must educate themselves on the technology, so that they can ask the right questions and properly assess the reliability of the new types of evidence presented in their courts. As recently stated by a minority in the Appeals Chamber, "[i]n times where it has become ever more difficult to distinguish facts from 'fake news', it is crucial that the judiciary can be relied upon to uphold the highest standards of quality, precision and accuracy."[271] In order to do this, the ICC Chambers may want to consider moving towards a more rigorous approach to admissibility of evidence and, where appropriate, have evidentiary hearings on the admissibility of digital evidence. Such an approach may mean excluding irrelevant and unreliable evidence, such as documents containing anonymous hearsay,

---

Ruto and Sang; and a forced decision to drop charges in *Kenyatta*. Another no case to answer motion is pending in *Gbagbo*. Labuda, *supra* note 260.

270. PATRIKARAKOS, *supra* note 54, at 25.

271. Bemba Appeal Separate Opinion, ICC–01/05–01/08–3636–Anx2, Separate Opinion of?Judge Christine Van den Wyngaert & Judge Howard Morrison, ¶ 5 (June 8, 2018).

rather than admitting a wider range of items of evidence with little weight that ultimately crowd the case record and add little value.[272]

B. *Extraterritorial Investigations*

While digitally distributed false narratives around war may obstruct the fact-finding process, tracking the source of distribution and proving attribution can also benefit prosecutions. Propaganda or documented encouragement of criminal conduct may prove intent or other elements of crimes.[273] Cyberspace is borderless by nature and state-imposed regulations on internet use within a country's borders are often circumvented. The desire of individuals to connect freely across national boundaries is overpowering and states find it difficult to fight this strong will among the global civilian population.

Digital devices such as computers, surveillance cameras, smartphones, satellite phones, ground sensors, drones, and GPS devices are widely used in military operations and in civilian daily life. These devices record and accumulate significant amounts of data on hard drives, servers, or the cloud.[274] This digital data is generally thought to be closed-source, meaning that a subpoena, search warrant, or some other legal process is generally necessary for law enforcement to acquire such private materials. But unlike traditional closed-sources—such as files in a cabinet in a private residence—physical barriers to the acquisition of closed-source data do not exist, at least in the traditional sense. Previously, technological barriers were a limiting factor. However, as those barriers dissolve, only the law provides restrictions and protects privacy. When technical

---

272. Judges Van der Wyngaert and Morrison, writing separately on the Bemba Appeal, supported such an approach and asseted, "if this had been done in the present case, many of the problems that we have identified in this section would not have arisen." Bemba Appeal Separate Opinion, ICC–01/05–01/08–3636–Anx2, ¶ 18.

273. For example, in Prosecutor v. Nahimana, Case No. ICTR–99–52–T, Judgment and Sentence, ¶ (Dec. 3, 2003) [hereinafter Media Judgment and Sentence] the Trial Chamber found Nahimana guilty of direct and public incitement of genocide.

274. *See* MAURER, *supra* note 130, at 7 (noting that "more and more machines—including cars and control systems in industry—are changing from closed manual and mechanical systems to interoperable digital systems," and that, "more and more of these digital devices are connecting to the Internet.").

barriers vanish, the reality of digital evidence acquisition raises complex legal issues with implications for state sovereignty, individual privacy, data protection, and information security. The lack of borders and the nature of free-flowing data also raise questions about where data reside for the purposes of applicable laws and jurisdiction. In many cases, relevant data are held by third parties such as communications service provides (CSPs) or internet service providers (ISPs). This structure raises issues concerning ownership of data as well as legal ability and responsibility to provide it to governments and law enforcement in response to a request.

The lack of a supra-national governing structure over the internet presents complex legal questions regarding jurisdiction and disputes over the location of data. At the crux of most cyber governance debates is the need to balance concerns over national security and public safety against individual rights to privacy. States take very different approaches to the privacy versus security debate, and this divergence leads to conflicting laws over data protection and privacy rights in the digital age. The exchange of information relevant to criminal investigations between states is governed by mutual legal assistance treaties (MLATS).[275] When war crimes are investigated and prosecuted at the domestic level, national law enforcement use the MLAT process when requesting and collecting user data from servers located outside their jurisdiction.[276] For ICC investigators, Part IX of the Rome Statute, as well as separate cooperation agreements established on an ad hoc basis govern the exchange of information from states to the ICC. While these regimes for overseas data exchanges exist, there are several problems with their operation in practice. The MLAT process is inordinately slow and, in many cases, limited political

275. For detailed information on existing MLATs between different countries, see *Mutual Legal Assistance Treaties*, ACCESS NOW, https://www.mlat.info/ (last visited March 24, 2019).

276. *See* Alexa Koenig et al., *Access Denied? The International Criminal Court, Transnational Discovery, and The American Servicemembers Protection Act*, 36 BERKELEY J. INT'L L. 1, 32 (2018) ("Under the MLA regime, foreign countries that hope to acquire stored electronic communications and/or other digital data from private technology companies based in the United States and have an MLA treaty in place with the United States would make a request for assistance to the secretary of state, the U.S. attorney general, or their designees.").

will, or even outright opposition, obstructs state cooperation with the ICC.[277] The changing nature of electronic searches and the inefficacy of the current system necessitates a new legal framework for digital evidence acquisition.[278]

The digital landscape also presents new opportunities and challenges for investigators in the acquisition, storage, and preservation of digital evidence. This sub-section focuses on two legal debates arising recently in litigation and legislation with regard to law enforcement access to closed-source digital information: (1) accessing digital evidence that is held by a third-party; and (2) accessing digital evidence through a live-remote connection to a personal computer. These legal issues are particularly complex when the physical server or laptop is located outside the territory of the jurisdiction issuing the warrant. This section explores the important and contentious issues emerging in the cyber era regarding the legality of extra-territorial search warrants to seize electronic information stored on servers abroad and warrants that permit law enforcement hacking of personal digital devices when the devices are outside the issuing court's jurisdiction.

The landmark case of *United States v. Microsoft* famously raised the issue of access to digital data stored overseas.[279] This case considered whether the FBI could access an individual's digital data in the context of a transnational drug trafficking case. The FBI served a warrant on Microsoft headquarters in Washington state for information relevant to the investigation. Microsoft refused to comply, challenging the warrant on the basis that the emails were stored on servers in Ireland and, therefore, that producing the emails through their U.S. headquarters would violate Irish law and EU law. In support of their procedure and jurisdiction, the U.S. government relied on the

277. *See* Drew Mitnick, *What's Wrong with the System for Cross-Border Access to Data*, ACCESS NOW (Apr. 25, 2017), https://www.accessnow.org/whats-wrong-system-cross-border-access-data/ ("In short, the system is too slow, creating incentives for governments to develop rights-harming workarounds that damage our privacy.").

278. Erin E. Kenneally, *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live Remote Digital Evidence Collection*, 2005 UCLA J. L. & TECH. 5; *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85 (2005).

279. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

Stored Communication Act of 1986,[280] which pre-dated the public internet. The technology companies argued for clear legal authority because they did not want to be subject to inconsistent legal obligations.[281]

While the Supreme Court deliberated the case, the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018,[282] which amended the 1986 Storage Communications Act and made the Microsoft case moot. While the CLOUD Act is an improvement in terms of the clarity it provides, some argue that it went too far in granting law enforcement a path to make an end-run around the Fourth Amendment.[283] The *Microsoft* case also prompted new legislation in Europe—the EU General Data Protection Regulation (GDPR),[284] which takes a different approach to the protection of individual's data. There are three emerging global approaches to privacy in the digital age: (1) the European approach, which views individuals as the rights holders of their data;[285] (2) the U.S. approach, which views corporations as the rights holders of individuals' data;[286] and (3) the Russian and Chinese approach, which views the government as possessing the ultimate right to individuals' data.

Another pressing issue for modern criminal investigators is the legality of hacking by law enforcement—an activity that

---

280. *Id.* at 1187; *see also* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2701–2711 (2019)).

281. Samuel Noah Weinstein, *United States v. Microsoft Corp.*, 17 BERKELEY TECH. L.J. 273 (2002).

282. Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 115th Cong. (2018) (enacted in H.R. 1625, 115th Cong.).

283. For an example of such an argument, see Neema Singh Guliani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them*, LAWFARE (Mar. 16, 2018), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

284. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119).

285. *See* Franz-Stefan Gady, *EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis*, 2014 GEO. J. INT'L AFF.: INT'L ENGAGEMENT ON CYBER IV 12, 14 ("[U]nlike in the United States, where ownership belongs to the company or service that assembled the data, every individual has ownership of his data under European law.").

286. *Id.*

occurs when a law enforcement officer, with or without a warrant depending on the jurisdiction, remotely accesses a personal computer that may be inside or outside of a given jurisdiction and searches it with the intent to find evidence of a crime. Revelations from whistleblowers and legal cases before the European Court of Human Rights have revealed that several government intelligence apparatuses employ questionable methods of surveillance, but few people may be aware of the debate over legal hacking by law enforcement as a means of criminal investigation and electronic evidence collection. In response to increased encryption, law enforcement agencies all over the world acquire data, much of which resides across borders or belongs to non-nationals,[287] through hacking techniques. Since laptops are mobile and masking the location of such a device is easy with a VPN or TOR, a law enforcement officer may hack a machine without actually knowing the location of the physical device. This may lead to live-remote digital evidence acquisition, which does not require physical proximity to the target device.[288]

There have been four recent U.S. cases stemming from a FBI hacking operation conducted pursuant to a warrant issued by a federal judge.[289] The warrants authorized the use of network investigative technique, which is essentially a form of hacking, on a large number of computers, including many located outside U.S. territory. Proponents argue that permitting such activity is a practical adjustment to the current digital reality and allows law enforcement to keep up with criminality in the cyber age more effectively. Law enforcement entities generally argue that, in today's world, it is impossible to do the job of investigating illegal activity and prosecuting criminals without the ability to employ certain hacking techniques and acquiring relevant data through exploiting vulnerabilities in sys-

287. DIRECTORATE GEN. FOR INTERNAL POLICIES, EUROPEAN PARLIAMENT, LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION AND COMPARISON OF PRACTICES 8 (2017).

288. *See generally id.* (discussing the methodology and outcome of a study that focused primarily on the use of hacking to gain remote access to ICT systems).

289. *See* United States v. Levin, 874 F.3d 316 (1st Cir. 2017); United States v. Werdene, 883 F.3d 204 (3d Cir. 2018); United States v. Eure, 723 F. App'x 238 (4th Cir. 2018); United States v. Tippens, No. 16–cr–5110–RJB–1, 2017 U.S. Dist. LEXIS 219162 (W.D. Wash. Mar. 16, 2017).

tems.[290] Opponents, on the other hand, would point out that these activities present a challenge to traditional ideas of state sovereignty, as well as new risks to individual privacy.

Despite such opposition, in 2016, Rule 41 of the U.S. Federal Rules of Criminal Procedure was amended to allow judges to issue warrants allowing federal law enforcement agencies to use remote access tools to access computers outside the jurisdiction in which the warrant was granted.[291] This amendment effectively legalized the practice of law enforcement hacking. Similarly, the EU, France, Germany, Poland, and the UK also adopted legislative provisions permitting hacking practices, and similar laws in Italy and the Netherlands are in the legislative process.[292] The growth of legislation permitting these activities raises the question of whether ICC investigators could engage in similar activities under the framework of the Rome Statute and international law. These new investigative techniques raise questions about what the ICC can do legally and politically if the technical barriers that necessitate cooperation with states disappear. While it is indisputable that international criminal investigators face uniquely challenging circumstances that cannot be easily compared to the domestic law enforcement context, the ICC would nevertheless benefit greatly from learning from their national counterparts who are already experimenting and finding solutions to future problems. Finally, it is important to note that while these practices provide benefits to investigators in the face of an advanced threat and increasingly sophisticated criminality, they do present significant risks to fundamental rights, such as the internationally-recognized human right to privacy.[293]

---

290. *See, e.g.*, INT'L ASS'N OF CHIEFS OF POLICE, DATA, PRIVACY AND PUBLIC SAFETY: A LAW ENFORCEMENT PERSPECTIVE ON THE CHALLENGES OF GATHERING ELECTRONIC EVIDENCE 15 (2015) ("A significant percentage of communications content evidence and related data evidence have shifted *from* face-to-face, telephonic, cellular, or text message transport *to* Internet-based communications and remote storage. This evidence is becoming inaccessible to law enforcement because of barriers to access or obstacles that law enforcement faces in collecting digital and communications evidence. . . . With these changes, law enforcement's ability to protect the public is diminishing.").

291. FED. R. CRIM. P. 41(b)(6).

292. DIRECTORATE GEN. FOR INTERNAL POLICIES, *supra* note 287, at 10.

293. Article 8 of the European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his corre-

C. *Modernizing International Criminal Procedure*

The chief check to balance the use of hacking techniques by investigators is the right to privacy.[294] The right to privacy is a fundamental human right[295] and one that will need to be reassessed and applied to novel factual scenarios by judges. The state-centric system of international law established in the wake of World War II is, as Chinkin and Kaldor put it, "out of step with the changing nature" of the world and is decreasingly relevant as technology makes citizens less reliant on and less easily controlled by their governments.[296] The authors present the argument that the decreased importance of sovereignty is a direct result of technology, which allows citizens to circumvent traditional state power over the flow of information.[297] The world still has physical boundaries, but its data does not. Data is typically stored where it is most technologically convenient and cost effective. Efforts to force data localization laws are likely to be unsuccessful and ineffective,[298] as data localization will give rise to a more expensive, less efficient, and less secure internet. When physical and technical barriers disappear, only the law is left to provide privacy protection in the digital age. Legal efforts are complicated by the very nature of data and the ways in which its fluidity across jurisdictions challenges long-standing notions of sovereignty. Against this complexity, international organizations must de-

---

spondence," subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society." European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, E.T.S. No. 5.

294. MIRJA GUTHEIL ET AL., LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION AND COMPARISON OF PRACTICES 8 (2017) ("Hacking by law enforcement is a relatively new phenomenon within the framework of the longstanding public policy problem of balancing security and privacy.").

295. European Convention of Human Rights art 8, Nov. 4, 1950, E.T.S. No. 5, 213 U.N.T.S. 221.

296. CHINKIN & KALDOR, *supra* note 2, at 37.

297. "De-territorialised actions like those taken in cyberspace have led to the erosion of traditional views of sovereignty." *Id.* at 56.

298. Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet* (U.C. Davis Legal Studies Research Paper Series No. 378, 2014) (discussing concerns raised by and impediments to global data localization requirements).

velop and maintain a consistent approach to the legal use of data.

At the national level, criminal investigators rely on state powers to acquire privately held digital evidence in accordance with procedures such as applications for search warrants based on probable cause or subpoenas. Although national law enforcement, pursuant to a valid search warrant, may employ live-remote acquisition techniques on computers and other devices located anywhere in the world, it remains unclear whether the same standard applies to international criminal investigators. International criminal investigators do not have the same legal coercive powers or mechanisms as national law enforcement and, therefore, face enormous obstacles when collecting evidence. Whether it is locating and interviewing witnesses or gathering documents and physical evidence, ICC investigators must navigate many legal, technical, and physical restraints. Arguably chief among them is the fact that the Prosecutor's ability to collect evidence is entirely reliant on the cooperation of member states—cooperation which to date has been deficient or non-existent.[299]

Given these new realities, the overall framework will change. Looking ahead, the ICC would be wise to pay close attention to developments in the law like the EU GDPR and U.S. CLOUD Act. Further, as technologies become more complex and governments try to maintain a tight hold on military dominance, the ICC will likely meet resistance from states asked to provide evidence and foundational information about technologies. States might hide behind national security privilege in order to protect sources and means or come up with other legal justification for refusing to cooperate. The Prosecutor must prepare for such resistance.

One way to protect use of experimental cyber investigative techniques is through Article 56 of the Rome Statute, which enables the Pre-Trial Chamber to approve of these active mea-

299. *See* KENYANS FOR PEACE WITH TRUTH & JUSTICE, ALL BARK, NO BITE?: STATE COOPERATION AND THE INTERNATIONAL CRIMINAL COURT 24 (2014), http://kptj.africog.org/wp-content/uploads/2015/02/FINAL-ICC-COOPERATION-210215.pdf ("With no enforcement agency at its disposal, the ICC cannot execute arrest warrants, compel witnesses to give testimony, collect evidence or visit the scenes where the crimes were perpetrated, without the acquiescence of national state authorities.").

sures.[300] This would require ICC investigators to articulate why certain investigative techniques are necessary based on the circumstances of the case, engage the judges in the investigative process so they truly understand the hurdles, and ultimately provide judicial support for the methods employed. If legally permissible, exploiting technology through means such as improving open source investigation techniques and live-remote hacking could drastically improve ICC investigative capabilities.

VI. CONCLUSION

In the modern era, the laws of conflict cause conflicts of law. The ICC is a relatively young institution, which has had to fight for its existence and establish its credibility and legitimacy on the global stage.[301] This has been an ongoing struggle, especially in the context of current geopolitics, a trend towards nationalism, and mounting criticism of the Court. Despite several recent setbacks,[302] the ICC must continue demonstrating its relevance and efficacy when dealing with contemporary armed conflicts. A major element of this effort to stay relevant and effective involves tackling the challenges posed by technology and twenty-first century warfare. It is vitally important for the institution that its stakeholders grapple with these pressing issues as soon as possible. Judges must take a clearer, more decisive approach to admissibility of evidence. A stricter approach to evidence and clearer procedures will benefit all parties, even the Prosecutor, who will be forced to focus on the quality rather than the quantity of evidence and develop greater agility in the face of changing circumstances. The OTP

300. Rome Statute, *supra* note 33, art. 56; *see generally* Paul Bradfield, *Preserving Vulnerable Evidence at the International Criminal Court*, INT'L CRIM. L. REV. (Feb. 5, 2019) (explaining how Article 56 can be strategically used in the pre-trial stage of the case to preserve vulnerable evidence as exemplified in *Prosecutor v. Ongwen*).

301. *See generally* Yvonne M. Dutton, *Bridging the Legitimacy Divide: The International Criminal Court's Domestic Perception Challenge*, 56 COLUM. J. TRANSNAT'L. L. 71 (2017).

302. During the writing of this article, the conviction of Bemba was overturned on appeal and the Trial Chamber found that there was no case to answer in *Prosecutor v. Gbagbo and Blé Goudé*. *See* Luke Moffett, *Why Gbagbo Acquittal is a Bigger Blow for the ICC than the Bemba Decision*, CONVERSATION (Jan. 15, 2019), https://theconversation.com/why-gbagbo-acquittal-is-a-bigger-blow-for-the-icc-than-the-bemba-decision-109913.

should consider using all tools available, which may include making more use of the Pre-Trial Chamber during the investigation stage. When there is doubt and confusion over permissible investigative techniques, there should be a mechanism for the judges to weigh in.

Although IHL provides a foundation for the war crimes codified in the Rome Statute, judges should not be strictly bound by the Geneva Conventions, but rather interpret the Statute as is appropriate with the changing times. The Rome Statute should not be strictly construed to adhere to every classification, requirement, and definition in IHL—particularly if parts of IHL are not explicitly stated in the Statute. Further, the judges should readily invite the knowledge, experience, and input of military and technical experts who are in touch with current circumstances on the ground. The Court requires expertise from people who truly understand relevant technologies and will have to rethink outdated assumptions about the nature of modern fighting forces, especially the chain of command in militaries and organized armed groups.

Perhaps the most important message to take from this article's inquiry is that it is not too early to consider these issues. On the contrary, without immediate, decisive action it could quickly become too late. Every section of this article supports and recommends ongoing research and more thorough analysis. In order to support and accomplish the OTP's investigations in, for example, Georgia, Darfur, and Libya, or preliminary examinations in Ukraine, Palestine, Bangladesh/Myanmar, and Venezuela, the Prosecutor must focus on techniques that ensure that digital information is properly preserved and verified while installing proper safeguards to protect the internationally recognized human right to privacy.

In the ICC's two decades of existence, war has incontrovertibly and dramatically changed. Instead of theoretically examining how the laws of war apply to new technologies, the global community must start talking more practically about how technological changes require amendment of the laws and, further, how changes on the battlefield might transform the investigation process and courtroom procedures. The value, legitimacy, and relevance of the ICC and international criminal justice more generally depends on it.