Weapons of War, Tools of Justice

Using Artificial Intelligence to Investigate International Crimes

Lindsay Freeman*

Abstract

Just as the internal combustion engine revolutionized warfare in the early twentieth century, artificial intelligence is shaping warfare in the Digital Age. Fuelled by data rather than gasoline, artificial intelligence (AI) derivative technologies are driven by innovation in both the military and civilian sectors. Today's defence scientists and engineers, like their predecessors, develop physical equipment and weapons, but instead of simply making them more powerful and lethal, they are also making them more intelligent and connected. As AI is increasingly integrated into military tools, the digital footprints of modern battlefields will grow exponentially, generating new sources and types of data that will fundamentally alter war crimes investigations. This article examines emerging military applications of AI in order to identify what opportunities and challenges these tools might offer international criminal investigators. Will more sensors and smart devices on the battlefield benefit or burden the investigation of war crimes? Moreover, will intelligent machines add to the fog of war or help us see through it?

1. Introduction

> *The next war may never come. It is conceivable that the protocol of arbitration and security, now being negotiated through the League of Nations, may provide a means of escape from ultimate*

* Lindsay Freeman is the Law and Policy Director of the Technology and Human Rights Program at Human Rights Center, UC Berkeley School of Law (USA). She is a member of the Pacific Council on International Policy, the ABA International Criminal Justice Standards Advisory Group, and the Technology Advisory Board of the Office of the Prosecutor of the International Criminal Court. The views in this article are those of the author alone. The author would like to thank Alexa Koenig, Daragh Murray, Raquel Vazquez Llorente and the *JICJ* editorial team for their thoughtful and invaluable feedback, guidance and support. [lfreeman@berkeley.edu]

Journal of International Criminal Justice **19** (2021), 35–53 doi:10.1093/jicj/mqab013
Advance Access publication 23 March 2021

catastrophe of physical conflict ... but if international conflict is again renewed the violence of the late World War may seem by puny effort in contrast with the tremendous forces that men will utilize in order to impose their will upon 'the enemy'.[1] — William L. Chenery (1924)

The New York Times published this prescient message of hope, tempered by caution, on the 'New Tools of War' in 1924.[2] Written by journalist William L. Chenery, this article revealed significant advances in military research, highlighting specific technologies of the era, including tanks, airplanes, anti-aircraft missiles, .50-caliber machine guns, demolition bombs, and weaponized poisonous gases. With each emerging technology, Chenery described its development and potential applications in a future war, should another global armed conflict arise. World War II broke out 15 years after these words were written, making Chenery's warning all too real. In 1924, tools for war were being built and refined for ever-greater movement and strength of force. Quoting Major General C.C. Williams, Chenery explained that the demand of the future required making weaponry more mobile, more powerful, and more deadly.[3] In his research for the article, Chenery observed an interesting paradox in the dual lines of inquiry then-being pursued by ordnance inventors. Scientists dedicated to creating the deadliest weapons were also improving the means of protection against them. Artillery experts crafted bullets to penetrate existing armour in parallel to fashioning armour strong enough to prevent penetration. Engineers manufactured anti-aircraft weapons to bring down airplanes, while at the same time making powerful aircraft weapons to render those airplanes even more lethal. Chemists cultivated toxins and their antidotes. Chenery noted, in particular, the innovation of the tank — a tool that could be used both to destroy and to defend. It was, at once, the sword and the shield.[4]

While the tools of war reported on by Chenery do not appear immediately relevant to modern war crimes investigations, Chenery's accurate forecasting of future warfare based on his examination of contemporary defence research and development projects offers a compelling framework for international criminal investigators to anticipate and prepare for the challenges ahead. Today, nearly a century after Chenery's writing, defence research and development projects have shifted their focus from the kinetic world to the digital one. Instead of simply making tools of war more powerful and deadly, today's military scientists and engineers are also making them more intelligent and connected.[5] The same paradox observed by Chenery continues today. Cryptographers developing the next generation of military-grade encryption are also developing sophisticated software to break advanced encryption.

[1] W.L. Chenery, 'New Tools of War Outstrip Those of 1918', *The New York Times*, 12 October 1924, available online at https://timesmachine.nytimes.com/timesmachine/1924/10/12/issue.html (visited 19 January 2021), at 185.

[2] *Ibid.*

[3] *Ibid.*

[4] *Oxford Dictionary* defines 'tank' as 'a heavy armoured fighting vehicle carrying guns and moving on a continuous articulated metal track'. Thus, the tank is armed and armoured.

[5] R. Sammon, '8 Amazing New Military Technologies', *Kiplinger*, 29 December 2016, available online at https://www.kiplinger.com/slideshow/business/t057-s010-amazing-military-technologies/index.html (visited 19 January 2021).

Internet researchers search for new ways to deanonymize data while trying to maintain their own anonymity when searching for data online.[6] Engineers working on digital image authentication tools to identify digital manipulation are, at the same time, improving the algorithms used for creating fake images and videos.[7] Increasingly, military researchers are using generative adversarial networks (GANs), which are deep neural networks that are 'able to learn from a set of training data and generate new data with the same characteristics as the training data'.[8] This process illustrates beautifully Chenery's paradox, as when two neural networks are pitted against each other in order to simultaneously develop, for example, an algorithm that can detect synthetic images and an algorithm that can generate synthetic images that evade detection.[9] Like the tank, artificial intelligence can serve as both sword and shield.

Experts predict that 'conflict in the future will take place in a battlespace that is shaped by artificial intelligence and other new technologies.'[10] Just as the internal combustion engine led to numerous derivative technologies that shaped the character of war a century ago — including aircrafts, submarines, and tanks — derivative technologies of artificial intelligence — including machine learning, natural language processing, image recognition, biometrics, robotic process automation, content creation, and cyber defence — are already shaping the way war is waged in the Digital Age.[11] Partnerships between government militaries, defence contractors and technology companies signal that future battlefields will be filled with smart devices and sensors,[12] and defence spending by major powers

[6] UC Berkeley Human Rights Center and Office of the High Commissioner of Human Rights, *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law* (2020), available online at https://www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf (visited 15 February 2021), at 41–42 (hereafter 'Berkeley Protocol').

[7] See generally T. Thi Nguyen et al., 'Deep Learning for Deepfake Creation and Detection: A Survey', 28 July 2020, available online at https://arxiv.org/pdf/1909.11573.pdf (visited 15 February 2021), at 1–12.

[8] T. Wood, 'What is a Generative Adversarial Network, DeepAI', *Deep AI*, available online at https://deepai.org/machine-learning-glossary-and-terms/generative-adversarial-network (visited 19 January 2021).

[9] Synthetic media describes media — including videos and images — that is either algorithmically created or modified. See also Pathmind, 'A Beginner's Guide to Generative Adversarial Networks (GANS)', *A.I. Wiki*, available online at https://wiki.pathmind.com/generative-adversarial-network-gan#:~:text=Generative%20adversarial%20networks%20(GANs)%20are,video%20generation%20and%20voice%20generation (visited 19 January 2021).

[10] P.L. Hickman, 'The Future of Warfare Will Continue to be Human', *War on the Rocks*, 12 May 2020, available online at https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/ (visited 19 January 2021).

[11] 'Top 15 Hot Artificial Intelligence Technologies', *Blog of Edureka*, 2 January 2020, available online at https://www.edureka.co/blog/top-15-hot-artificial-intelligence-technologies/ (visited 19 January 2021).

[12] S. Gibbs, 'Google's AI is being used by US Military drone program', *The Guardian*, 7 March 2018, available online at https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow (visited 19 January 2021); A. Eversden, 'Palantir wants to be the 'central operating system for all US defense programs'',

reveals a collective recognition that competitive advantage in future wars will go to the smartest, not just the strongest.[13] Thus, while the weapons deployed in World War II did not offer much in the way of helpful tools for war crimes investigators, modern military technology may, in fact, prove as useful to those fighting for justice as they do for those fighting wars.

Inspired by Chenery's insights of nearly a century ago, this article takes a deep look at current military research efforts concentrated on the application and integration of artificial intelligence (AI) in tools of war. This article examines how AI is being incorporated into military weapons, equipment, vehicles, infrastructure and systems in order to: (1) improve strategic intelligence capabilities with machine-enhanced data collection and analysis; and (2) improve tactical deception capabilities with machine-enhanced data manipulation. Furthermore, this article contemplates how the increased use of AI derivative technologies in warfare might impact those seeking justice and accountability for violations of international humanitarian law and international criminal law (IHL/ICL). It examines whether and how war crimes investigators will be able to utilize data collected and processed by sensors and smart devices on the battlefield, and whether the use of AI to create and spread disinformation during military operations will impede investigators in their search for the truth.

Finally, this article points to examples of how similar applications of AI, particularly enhancing image and object recognition through machine learning, are being integrated into current war crimes investigations. AI has great potential to assist in the investigation and prosecution of war crimes and other violations of international law, but it will also inevitably create new obstacles for those in pursuit of justice and accountability. Therefore, international criminal justice institutions and practitioners must prepare to address these emerging challenges by anticipating and understanding how AI technologies are changing the character of warfare and the character of war crimes investigations.

2. Computer-generated Intelligence

Chinese military strategist Sun Tzu wrote in *The Art of War*, 'It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for the purposes of spying, and thereby they achieve great results.'[14]

C4isrnet, 30 September 2020, available online at https://www.c4isrnet.com/industry/2020/09/30/palantir-wants-to-be-the-central-operating-system-for-all-us-defense-programs/ (visited 19 January 2021); D. Goldstein and G. Gordon, 'Documents could Link Russian Cybersecurity Firm Kaspersky to FSB Spy Agency', *Chicago Tribune*, 3 July 2017, available online at https://www.chicagotribune.com/nation-world/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html (visited 19 January 2021).

[13] C. Pellerin, 'Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence', US Department of Defense, 31 October 2016, available online at https://www.defense.gov/Explore/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/ (visited 19 January 2021).

[14] S. Tzu and S. Griffith, *The Art of War* (Clarendon Press, 1964).

His insight underscores the great importance of intelligence tradecraft in achieving military victories. In the same text, General Sun Tzu later writes, ‘All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.’[15] His guidance highlights the tactical utility of deceit and disinformation in warfare. This article examines the use of AI to further both aims, with this section focused on the use of AI for intelligence purposes and the following section focused on the use of AI for deception purposes. This section explores technological innovations that illustrate how AI derivative technologies can and are being integrated into military objects and equipment to improve situational awareness and operational intelligence. Using concrete examples of AI in military intelligence, this section explores how such new and emerging technologies might impact the investigation of war crimes and, further, whether war crimes investigators might be able to utilize the same technologies to their own advantage.

A. Data as Weapons of War

The goal of maximizing intelligence in warfare is not new.[16] The US Department of Defense defines military intelligence as ‘a military discipline that uses information collection and analysis approaches to provide guidance and direction to assist commanders in their decisions’.[17] There are many different types of intelligence — including human intelligence (HUMINT), signals intelligence (SIGINT), geospatial intelligence (GEOINT) and open-source intelligence (OSINT) — that have long been an important part of armed combat strategy, and technological innovation has long been an integral part of intelligence work. However, emerging digital technologies in recent years have led to a novel type of military intelligence: machine intelligence. Machine intelligence (MACHINT) involves the automated collection, processing, analysis and interpretation of multi-source data by machine learning algorithms rather than human analysts.[18] In the past, the greatest challenge to military intelligence was the ability to obtain enough data, so researchers concentrated on finding better ways to access more data.[19] In today’s age of

[15] *Ibid.*

[16] Sun Tzu’s *The Art of War* is believed to have been written between 475 and 221 B.C.E. see ‘The Art of War’, *National Geographic*, available online at https://www.nationalgeographic.org/encyclopedia/art-war/#:~:text=It%20is%20hard%20to%20know,during%20the%20Warring%20States%20period (visited 17 February 2021). See J. Keegan, *Intelligence in War: The Value–and Limitations–of What the Military can Learn about the Enemy* (First Vintage Books Edition, October 2004).

[17] DOD Dictionary of Military and Associated Terms, available online at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (visited 21 February 2021).

[18] A. Roland and P. Shiman, *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993* (The MIT Press, 2002), at 1 and 285.

[19] N. Lopez and K. Atwell, ‘Artificial Intelligence in Counterterrorism and Counterinsurgency, with Retired Gen. Stan McChyrstal and Dr. Anshu Roy’, Modern War Institute at West Point, 1

information, where there is an overabundance of intelligence sources, the key challenge has moved from data scarcity to data overload. The novel challenge is finding a way to effectively organize, analyse and interpret all that data. While technologists continue to work on enhancing the ability to collect more data with new technologies, defence professionals are more focused on technologies that can process data at a speed and with a level of accuracy that enables operational decision-making in real-time.

One emergent area of military research and development is the Internet of Military Things.[20] The Internet of Things (IoT) is a system of interconnected computing devices, algorithms, and physical objects with unique identifiers that can transfer data over a network without any human intervention, thus enabling autonomous data processing.[21] Gartner, a global IT research firm that publishes annual technology forecasting reports, describes the IoT as a 'network of physical objects that contain embedded technologies to communicate and sense or interact with their internal states or the external environment'.[22] The IoT encompasses a broad range of products — not only smartphones and computers, but also automobiles, televisions, clothing and accessories, home heating, audio and security systems, refrigerators, pacemakers, gaming consoles, and even children's toys.[23] Former Cisco researcher David Evans explains that the network is also starting to include biological things like pets, crops, livestock, and humans.[24] AI is increasingly being integrated into IoT devices to provide insights from the data and support decision-making without human involvement. Experts estimate that there were roughly 31 billion devices connected to the internet as of 2020 and at

January 2021, available online at https://mwi.usma.edu/artificial-intelligence-in-counterterrorism-and-counterinsurgency-with-retired-gen-stan-mcchrystal-and-dr-anshu-roy/ (visited 21 February 2021).

[20] This article intentionally stays away from a discussion of automation and AI in the development of weapons and arms. Despite very few autonomous robotic weapons in use in combat today, many countries are developing and testing this capacity, and many academics are focusing on it. There is an uneven amount of scholarship dedicated to the dilemma of regulating lethal autonomous weapons compared to their usage, whereas very little has been written in international humanitarian law scholarship about the impact of other applications of automation and AI off the battlefield. Therefore, this article does not explore the use of the technology in arms, but rather focuses on its use in other types of military tools.

[21] J.Y. Khan and M.R. Yuce, *Internet of Things (IoT): Systems and Applications* (CRC Press, 2019), at 1.

[22] https://theinternetofthings.report/whitePapers/cybersecurity-and-the-internet-of-things/261 (visited 21 February 2021).

[23] Unicef Innovation and Human Rights Center, UC Berkeley School of Law, 'Executive Summary: Artificial Intelligence and Children's Rights', Unicef, 21 May 2019, available online at https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf (visited 17 February 2021).

[24] Through both wearables and implants. D. Evans, 'The Agenda: Introducing the wireless cow', *Politico*, 29 June 2015, available online at https://www.politico.com/agenda/story/2015/06/internet-of-things-growth-challenges-000098/ (visited 17 February 2021).

least 10 billion more will be connected to the IoT by 2027.[25] Gartner predicts that by 2022, more than 80 percent of enterprise IoT projects will include an AI component, up from only 10 percent in 2020.[26]

The Internet of Military Things (IoMT) is the application of IoT technologies and concepts to the military domain.[27] There are clear benefits for armed forces in the application of IoT devices for combat and non-combat activities including vehicle maintenance, personnel monitoring, and stock control.[28] The IoMT connects ships, planes, tanks, drones, and operating bases in a cohesive network that increases situational awareness, aids risk assessment, and improves response time.[29] The United States military takes the concept even further with the idea of the 'Battlefield of Things', which is envisaged as 'thousands of dynamically composed devices with sensors across the battlefield, exploiting autonomy and artificial intelligence to provide situational awareness and meet mission goals.'[30] Using a combination of strategically placed sensors and hyper-automation,[31] IoMT devices can 'discover, analyze, design, measure, monitor and reassess information',[32] autonomously carrying out complex tasks traditionally performed by human soldiers.[33] There is a great value in replacing human data collectors with autonomous machines, particularly in terms of security and resources. Instead of using human sentries or scouts, sensors can provide crucial data to the frontline from a great distance. In this context, AI could be used to rapidly aggregate, analyse and visualize hundreds of thousands of data points and even make recommendations that can inform decision-making during combat operations. For example, AI could use data from sensors collecting information on weather conditions, troop movements, civilian presence, ground conditions and other factors, paired with similar historical data, in order to predict and pre-empt an enemy's next move.

[25] K. Gyarmathy, 'Comprehensive Guide to IoT Statistics You Need to Know in 2020', Blog for vxchnge, 26 March 2020, available online at https://www.vxchnge.com/blog/iot-statistics (visited 17 February 2021).

[26] D. Schatsky, 'Bringing the Power of AI to the Internet of Things', *Wired*, available online at https://www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things/ (visited 17 February 2021).

[27] A. Poulter, 'The Internet of Military Things', available online at https://www.c-iot.ecs.soton.ac.uk/sites/www.c-iot.ecs.soton.ac.uk/files/AndrewPoulter.pdf (visited 17 February 2021).

[28] P. Fraga-Lamas et al., 'A Review on Internet of Things for Defense and Public Safety', 16 *Sensors* (2016) 1–44.

[29] L. Cameron, 'Context Aware Ubiquitous Biometrics in Edge of Military Things', IEEE Cloud Computing, available online at https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt (visited 17 February 2021).

[30] 'Artificial Intelligence and National Security', Congressional Research Service, 26 August 2020, available online at https://fas.org/sgp/crs/natsec/R45178.pdf (visited 17 February 2021).

[31] Gartner 'hyper-automation', which is the sophisticated application of machine learning (ML) across a range of tools in order to automate human tasks.

[32] K. Panetta, 'Gartner Top 10 Strategic Technology Trends for 2020', *Gartner*, 21 October 2019 available online at https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/ (visited 17 February 2021).

[33] From reconnaissance to intelligence analysis to operational decision-making, the IoMT can greatly minimize the number of human soldiers needed on the battlefield.

Closely tied to the IoMT is the concept of the Networked Soldier — a human soldier with machine-enhanced capabilities connected to the IoMT.[34] The concept expands on the use of wearables and biometric devices as part of the IoMT, adding the additional component that the collected data is processed and interpreted in real-time using AI and fed back to the soldiers as actionable intelligence. In addition, this concept also incorporates human augmentation technologies, which are technologies that enhance human cognitive and physical experiences.[35] There are four main categories of physical augmentation — sensory, biological, brain, and genetic — in addition to various types of cognitive augmentation.[36] Traditional armed forces carry communications equipment and munitions, whereas future armed forces, as they are envisioned, will be strapped with internet-connected mobile devices, wearable power sources, sensors to monitor health and safety, and technologies to increase situational, optical,[37] and environmental awareness.[38] In order to make any of this data operational in real-time, AI is essential to process, transmit, analyse, and receive the enormous quantities of data that are produced by these systems.

If this vision of future war is realized, future soldiers and battlefields will have significantly larger digital footprints than ever before. Embedded digital devices capable of data monitoring, collection, and analysis could be exploited by international criminal investigators to establish the who, what, when, where, and how of events, should war crimes occur. These AI-driven developments in military innovation will produce big data where, theoretically, the precise geographic location and movement of every combatant and civilian will be tracked and recorded. Imagery from satellites, drones, CCTV, and body cameras will be integrated to provide a 360-degree view of the entire conflict space. There are initial examples of this seen in the Syria context, where visualization software has been used to reconstruct military attacks using CCTV footage, victims' phones, Go-Pro cameras worn by first responders like the White Helmets, and journalists who capture the aftermath.[39] Detailed

[34] Engineering simulation software company AnSys markets 'the connected soldier', including wearable electronics and sensors, connected to a communications network, integrated and controlled through cloud-based software, see 'Connected Soldier', *Ansys*, available online at https://www.ansys.com/campaigns/internet-of-things/connected-soldier (visited 17 February 2021).

[35] Panetta, *supra* note 32.

[36] Physical augmentation falls into four main categories: Sensory augmentation (hearing, vision, perception), appendage and biological function augmentation (exoskeletons, prosthetics), brain augmentation (implants to treat seizures) and genetic augmentation (somatic gene and cell therapy). Cognitive augmentation is being advanced through neurotechnologies in the civilian sector as well as the military. See, for example, Elon Musk's Neuralink, which is developing ultra-high bandwidth brain-machine interfaces to connect humans and computers.

[37] Enhanced optical awareness the Soldier Scentric Imaging via Computational Cameras (SCENICC).

[38] The benefit, it claims, is increased situational, environmental and health awareness.

[39] See Forensic Architecture for several examples of visualizations and digital reconstructions of airstrikes, chemical weapons and attacks on hospitals in Syria: 'Syria', *Forensic Architecture*, available online at https://forensic-architecture.org/location/syria (visited 17 February 2021).

environmental data, such as shifts in wind conditions, and personal data, such as the heartbeat and blood pressure of human soldiers, will be collected, processed, and stored. Perhaps most importantly, due to increased storage space in addition to increased data collection capacity, time-stamped digital communications — both oral and text-based — will be produced and even preserved. This includes orders and responses up and down the chain of command, which could serve as direct evidence of war crimes. This digital linkage evidence would be particularly valuable for investigators who often struggle with establishing the link between high-level perpetrators and crimes committed by lower-level troops on the ground.

All the data processed by the IoMT, however, will only be useful to war crimes investigators if they have the ability to aggregate, organize, analyse and interpret it. Thus, the data must be accessible, readable, understandable and explainable for investigators, lawyers and judges. This raises the key question: with the technical infrastructure and resources of various international courts and tribunals, national law enforcement agencies, commissions of inquiry and even non-governmental organizations, will any of this be possible?

B. Tools to Analyse, Interpret and Visualize

The sheer amount of data generated by the IoMT and Networked Soldiers, on top of the data generated by traditional digital devices like computers and nearby civilian mobile devices, is difficult for humans to comprehend, let alone review and analyse. Market-intelligence predicts that the sum of the world's collective data will eclipse 175 zettabytes by 2025.[40] As the IoMT grows, so too will the volume and complexity of the data available for military decision-making. Analysing big data requires machine-assistance,[41] because its four defining attributes — volume, velocity, variety and veracity — make human review and analysis impossible.[42] Computers are needed to examine large-scale data, capture and analyse data in motion, assess the different formats of data, and address the uncertainty of data. Analytics software is also needed to make sense of the data and reveal its value.

In order to make use of the data generated by the military technologies discussed above, war crimes investigators and prosecutors will need their own technical infrastructure, including software and hardware, to process, aggregate or disaggregate, analyse, and draw conclusions from the information

[40] R. Whaley, 'The Big Data Battlefield, Military Embedded Systems', Military Embedded Systems, 9 August 2019, available online at https://militaryembedded.com/ai/big-data/the-big-data-battlefield (visited 17 February 2021).

[41] *Oxford English Dictionary* defines big data as 'data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges'. For alternative definitions, see G. Press, '12 Big Data Definitions: What's Yours?', *Forbes*, 3 September 2014, available online at https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/?sh=28b0bd4113ae (visited 17 February 2021).

[42] 'The Four V's of Big Data', IBM Big Data & Analytics Hub, available online at https://www.ibmbigdatahub.com/infographic/four-vs-big-data (visited 17 February 2021).

in their possession. They will likely also need specialized software to intake the data at all. In addition, any organizations investigating war crimes will need knowledgeable and appropriately trained personnel to use the technology and oversee its functioning.[43] AI-integrated systems of IoTs — whether civilian or military — raise several questions. Specifically, what infrastructure will war crimes investigators need in order to make use of data generated by the IoMT?[44] Further, could war crimes investigators use their own IoT devices to collect relevant data?

AI derivative technologies that are already in use by investigators include natural language processing and image recognition developed by machine learning software. Natural language processing enables and enhances keyword searches of text-based digital documents, whereas image recognition enables a similar function for signs and symbols. For example, the Impartial, Independent, Investigative Mechanism on Syria (IIIM) uses software to scan through Arabic-language documents to identify insignia as well as keywords.[45] However, the ability to run text-based searches is not equally effective in all languages. In particular, documents written in languages that use different characters than the Roman alphabet, documents written in less common languages, and documents that contain phonetic notation of spoken-only languages present ongoing challenges. In many cases, the demand may not be high enough to incentivize private companies to develop these less-used features that would prove of great value to the entire international criminal justice sector. In addition, digital images and audio-video material cannot be easily searched at present, although there have been some exciting developments in this area in recent years.

For example, Benetech, a non-governmental organization that creates software for social good is working on this very issue. Benetech's JusticeAI platform is intended to 'turn conflict data into actionable evidence' by using AI to automate and improve the process of analysing and making actionable huge amounts of data, with a specific focus on the matching and deduplication of digital images and videos.[46] As part of Microsoft AI for Humanitarian Action project, Benetech is also developing systems to recognize cluster-munitions and other types of weapons in digital imagery.[47] Similarly, Syrian Archive has worked with VFRAME, a Berlin-based technology company, to enable

[43] Y. Ng, 'How to Preserve Open Source Information Effectively', in S. Dubberley, A. Koenig, and D. Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford University Press, 2020) 200–258.

[44] This article acknowledges but does not address the legal challenges for war crimes investigators in obtaining military data, although they are significant. The focus of this article remains on the technological challenges.

[45] R. Abdulrahim, 'AI Emerges as Crucial Tool for Groups Seeking Justice for Syria War Crimes', *Wall Street Journal*, 13 February 2021, available online at https://www.wsj.com/articles/ai-emerges-as-crucial-tool-for-groups-seeking-justice-for-syria-war-crimes-11613228401 (visited 15 February 2021).

[46] Benetech JusticeAI platform, available online at https://benetech.org/lab/ethical-ai-to-promote-justice/ (visited 17 February 2021).

[47] Abdulrahim, *supra* note 45.

machines to recognize images or sounds of specific weaponry.[48] Carnegie Mellon University's Center for Human Rights Science is exploiting AI for the purpose of investigating international human rights abuses with the Video Event Reconstruction and Analysis (VERA) system and Event Labeling through Analytic Media Processing (E-LAMP).[49] Taking a similar approach, Amnesty International's 'AI for good' program is experimenting with using AI for pattern recognition,[50] among other potential applications to its work. This type of automated pattern recognition could be a useful tool for international criminal investigators and prosecutors who may have to prove the systematic or widespread nature of certain crimes or the *modus operandi* of a specific perpetrator.

In addition to the analysis of digital images, videos and documents, war crimes investigators will need software that can make sense of big, multi-source data. Early attempts at using these tools and techniques in war crimes investigations are already underway. For example, Hala Systems uses natural language processing and machine learning to rapidly ingest open media data about reported airstrikes, which feeds into its tracking and prediction algorithms.[51] By combining data from external sources with real-time information from human observers and sirens connected to the internet, Hala has created a system to warn civilians of incoming air raids.[52] Similarly, Videre uses devices to collect data and provides at-risk groups in conflict zones with early warning alerts of physical and digital attacks.[53] AI technologies have assisted in tremendous advances in the ability to visualize diverse data sets. SITU Research and Forensic Architecture are experimenting with the application of AI in their work to visualize and reconstruct events such as the Euromaidan protests in Ukraine.[54] While some commercial software is equally accessible to military analysts and war crimes investigations, such as graphical link analysis tools like Maltego and IBM's I2 Analyst Notebook, much of the software available to international criminal and human rights investigators is a far cry from what is being used by professional militaries.

In armed conflicts, image recognition technology is used to identify potential threats and risks in advance such as improvised explosive devices. In war crimes investigations, the same technology is used to identify objects in the

[48] *Ibid.*

[49] Technology Program, Center for Human Rights Science, Carnegie Mellon University, available online at https://www.cmu.edu/chrs/technology_program/index.html (visited 17 February 2021).

[50] S. Shetty, 'Artificial Intelligence for Google', Amnesty International, 9 June 2017, available online at https://www.amnesty.org/en/latest/news/2017/06/artificial-intelligence-for-good/ (last visited 15 February 2021).

[51] Hala Systems website available online at https://halasystems.com/ (visited 17 February 2021).

[52] O. Haj Kadour with J.M. Mojon, 'Air Raid Warning Tech Gives Syrians Life-saving Minutes', Phys org, 30 August 2018, available online at https://phys.org/news/2018-08-air-raid-tech-syrians-life-saving.html (visited 17 February 2021); S. Dadouch, 'Air Strike Warning App Helps Syrians Dodge Death from the Skies', *Reuters*, 13 September 2018.

[53] Videre website, available online at https://www.videreonline.org/ (visited 17 February 2021).

[54] SITU Research website, available online at https://situ.nyc/research/projects/euromaidan-event-reconstruction (17 February 2021).

aftermath of the attack, such as the shrapnel of an exploded device. The same algorithms used to distinguish civilians from combatants before an attack could be used to identify those differences in causalities afterward.[55] In order to create effective AI, data is needed to train it — good data, and lots of it. Once the AI is trained, it can be used to make sense of unknown data sets based on what it has learned. For example, if investigators need to identify a specific type of munition in images, they first have to teach the AI what these munitions look like using lots of data that reliably depict them. Human resources are also essential in this training process to confirm the accuracy of the AI as it is being trained. Only then can the AI be deployed to make correct identifications in the future. At present, investigators rely on the help of universities and non-governmental organizations, but they also might well be reinventing the wheel, as the military already has trained its AI to make these identifications.[56] Despite a clear recognition of the need to improve technological capacity,[57] international investigating entities have struggled with the ability to adopt such technologies. Many experts have pointed out the inherent tension between the rigid bureaucracy of international organizations combined with the cautious nature of the legal profession and the flexibility and efficiency needed to adopt new technologies.[58] Such endemic hurdles to innovation need to be addressed in order to properly navigate the technological possibilities for investigating modern warfare.

Understanding that future wars will come with a tremendous amount of data produced by sensors in the environment and on armed forces personnel and equipment means that war crimes investigators will be dealing with very different types of evidence than they encounter today. In order to adequately prepare for this contingency, investigators and lawyers must address a few essential questions. If investigators are going to use military-generated data as evidence, they will have to understand what type of legally relevant data is being generated by these new technologies, as well as where and how it is being stored and preserved. They will also need a channel through which to request and access the data, which is likely to be accompanied by legal and

[55] While AI can be used to distinguish civilians from combatants before an attack by military, and after by investigators, there will inevitably be cmplicating factors, such as situations involving non-uniformed fighters participating in hostilities. For example, military AI will presumably rely on a combination of image recognition and other intelligence sources to identify individuals as combatants or members of an armed group, but not all of the intelligence available to the military will be available to war crimes investigators.

[56] Z. Yang et al., 'Deep Transfer Learning for Military Object Recognition under Small Training Set Condition', 31 *Neural Computing and Applications* (2019) 6469–6478.

[57] Office of the Prosecutor, International Criminal Court, 'Strategic Plan 2019-2021', 17 July 2019, available online at https://www.icc-cpi.int/itemsDocuments/20190726-strategic-plan-eng.pdf (visited 15 February 2021).

[58] E. Piracés and J. Aronson, 'The OTP and ICC Can Take Advantage of Open Source Evidence and Digital Evidence Repositories, Core Elements of Almost All Grave Crimes Investigations, if They Undertake Cultural, Procedural, and Bureaucratic Changes to Create a More Agile and Open Institutional Environment', ICC Forum, June 2020, available online at https://iccforum.com/cyber-evidence#Aronson (visited 15 February 2021).

political challenges of cross-border data sharing, such as privacy and data protection laws, in addition to technical challenges. All these questions need to be worked out in advance because of the resources and time it will take to build the proper infrastructure and corresponding workflow. A key challenge, of course, is how to encourage bureaucrats to solve a problem they are not yet facing.

To date, most war crimes investigations and prosecutions have relied heavily on testimonial and documentary evidence, with a steep increase in geospatial and audio-visual evidence in recent years.[59] If the additional data sets of the IoMT corroborate these other types of evidence, it will certainly strengthen such cases. However, if there are inconsistencies between the data and witness accounts, already difficult cases will be even more challenging to prove beyond reasonable doubt. The digital records produced by these new and emerging technologies could allow for accurate and detailed event reconstruction and compelling visualizations that could prove incredibly useful in assisting factfinders at trial. However, whether the data can be utilized in this way is still an open question. Setting aside issues of access to this data, which will inevitably be a challenge for international institutions that rely heavily on state cooperation for evidence collection, international prosecutor's offices will need the technical capacity, both in terms of human resources and infrastructure, to process and make sense of this data while maintaining its authenticity, integrity and chain of custody.

3. Computer-generated Deception

In addition to his famous maxim quoted above — *all war is based on deception* — Sun Tzu has instructed, 'Engage people with what they expect; it is what they are able to discern and confirms their projections. It settles them into predictable patterns of response, occupying their minds while you wait for the extraordinary moment'.[60] Despite the many centuries that have passed since this writing, it describes perfectly the modern phenomenon of the internet's confirmation bias. Indeed, the orders given at Russian troll farms to launch information operations before the 2016 US Presidential election probably carried a similar sentiment. Disinformation and forgeries are not new, but AI is increasing the quality and volume of fake content exponentially. AI technologies are increasingly being deployed to forge and to fake, to manipulate and misinform, and to deceive and disinform. This section examines applications of AI in military research and development projects to improve tactical deception capabilities. While AI can be used to generate synthetic data and obscure facts about an armed conflict, there are several countermeasures being developed to detect synthetic data and identify digital manipulation. If future militaries are

[59] L. Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', 41 *Fordham International Law Journal* (2018) 283.

[60] Tzu, *supra* note 14.

going to use technology to generate synthetic data for strategic advantage, future war crimes investigators are going to need technology to determine what can be relied on and what cannot.

A. Lies as Weapons of War

While military science and technological development is heavily focused on using AI for the purpose of increasing intelligence capabilities, similar research efforts are equally dedicated to exploiting AI in order to manipulate, deceive, and confuse enemy forces. Indeed, AI derivative technologies are increasingly being used to generate deepfakes and synthetic media, spreading disinformation at speed and scale. These AI applications are employed for the purpose of masking the activities and strategies of armed forces, as well as enhancing information warfare. Lieutenant Colonel (Retired) Scott Padgett explains that 'state actors are using advanced software development tools and artificial intelligence (AI) to invent and perfect new deception capabilities to fool both people and machines on the virtual battlefield'.[61] Padgett illustrates this point with examples of the Russian government's evolving use of AI in disinformation campaigns including the annexation of Crimea from Ukraine in 2014 and the spreading of the Trojan Horse Narrative — a disinformation campaign asserting that international humanitarian aid was a cover for illegal arms imports — in the midst of armed conflict in Venezuela in 2019.

Padgett recounts how, in 2014, Russia sent a 'destabilization cell' into Ukraine to spread disinformation and stage fake protests, using actors who were recruited and trained to promote the pro-Russian movement.[62] Using this disinformation tactic as an example, Padgett explores how this could have been done with AI: 'If the Russians had intelligent computer vision systems to manipulate and synthesize audiovisual content in 2014, how would they most likely employ them and to what benefit?' This hypothetical raises a frightening scenario where fake events and synthetic characters could be digitally generated to serve this purpose at a much lower cost and with significantly less risk:

> News video of protests could be digitally altered to show thousands of protesters versus hundreds. Prominent adversarial politicians could be superimposed as protesters that would be easily recognized in the protests. Opposition leader comments in fake news interviews could be fabricated to alter opinions and facts. Instead of using mockups, they could digitally create synthetic military engagements that never happened on the kinetic battlefield.[63]

In 2019, the same Russian troll factories deployed similar tactics with the assistance of AI to automate the creation and distribution of content in Venezuela, spreading the Trojan Horse narrative, which alleged that

[61] S. Padgett, 'The Art of Digital Deception – Getting Left of Bang on Deep Fakes', *Small Wars Journal* (2019), available online at https://smallwarsjournal.com/jrnl/art/art-digital-deception-getting-left-bang-deepfakes (visited 15 February 2021).

[62] *Ibid.*

[63] *Ibid.*

humanitarian aid from the United States and international organizations were being used as cover to import illegal weapons to opposition groups. This false narrative was not only widely spread on social media but migrated from fake media sources to legitimate ones like the BBC.[64] Internet researchers found 3600 Spanish articles using this terminology from a combination of suspected bot accounts as well as reputable news media. While perhaps the boldest actor in this space, Russia is by no means the only state using these tactics.

In addition to the use of AI for content creation to fool humans, defence developers are also working on digital deception tactics to fool machines.[65] The digital operational environment described above with big data battlefields fuelled by the IoMT, while effective for military tacticians, creates new vulnerabilities for hacking, data poisoning, and other adversarial attacks. Colonel (Retired) Stefan Banach describes the concept of 'Synthetic Soldier Immunity', which is 'derived from the biological immune system of humans and is extrapolated into the Virtual Warfare construct in an attempt to protect Soldiers'.[66] The concept envisions three layers of protection for soldiers on future battlefields, one of which is 'active immunity'. This type of AI-developed immunity provides 'cloaking, spoofing, cloning, Bot warfare, electronic and signal intelligence, diversionary signatures, and virtual avatars—with physical footprints, to prevent Soldier detection'.[67] Such digital cloaking mechanisms have already been used on a smaller scale. For example, the United States Commerce Department regulates commercial satellite imagery providers and occasionally requires publicly distributed imagery to be blurred to obscure sensitive locations like military bases.[68] The ability to manipulate satellite imagery, which is heavily relied on for mapping armed conflicts, poses a real challenge for investigators. If that data is stored and later acquired by war crimes investigators looking into an incident, any manipulated information could distort investigators' understanding of relevant facts.

Other digital manipulation and cloaking techniques under development are not only designed for protection, but also as offensive countermeasures, such

[64] *Ibid.* 'On 22 February, Evo Morales, the President of Bolivia, uses the term in a statement quoted by RT, denouncing US humanitarian aid as a Trojan Horse. The same day, the BBC published an article with the headline "Venezuela aid: Genuine help or Trojan Horse?"'

[65] S.J. Freedberg Jr., 'Attacking Artificial Intelligence: How to Trick the Enemy, Breaking Defense', *Breaking Defense*, 6 February 2019 available online at https://breakingdefense.com/2019/02/attacking-artificial-intelligence-how-to-trick-the-enemy/ (visited 15 February 2021).

[66] Padgett, *supra* note 61.

[67] *Ibid.*

[68] M. Korda, 'Widespread Blurring of Satellite Imagery Reveals Secret Facilities', Federation of American Scientists, 10 December 2018, available online at https://fas.org/blogs/security/2018/12/widespread-blurring-of-satellite-images-reveals-secret-facilities/; https://www.livescience.com/60488-secretive-places-on-google-earth.html (last visited 17 February 2021); The Department of Commerce (Commerce), through the National Oceanic and Atmospheric Administration (NOAA), licenses the operation of private remote sensing space systems under the Land Remote Sensing Policy Act of 1992, see 'Licensing of Private Remote Sensing Space Systems' (US Federal Register), 20 May 2020, available online at https://www.federalregister.gov/documents/2020/05/20/2020-10703/licensing-of-private-remote-sensing-space-systems (visited 17 February 2021).

as the use of AI-supported visual effects software to alter images and videos in real time. The tedious work of photoshopping people and objects out of images is being replaced with intelligent tools that allow users to apply filters, delete unwanted elements in moving videos, and fill in a new background in milliseconds.[69] If visual sensors on the battlefield are not adequately protected, live streaming audio-visual data could be compromised, for example, to remove advancing forces from the moving picture. This software nullifies previously held assumptions about the time it takes to manipulate videos and images. Thus, while the comprehensive data with increased temporal and visual resolution produced by battlefield sensors and smart devices in the IoMT might provide war crimes investigators with a clearer picture of what transpired, the risk of digital manipulation and data alteration raises a huge concern about the ability to rely on such information as evidence in criminal trials.

B. Tools to Verify and Authenticate

While governments attempt to mitigate the impacts of disinformation campaigns originating in Russia and from other adversaries for military purposes, international criminal investigators must attempt to properly identify and analyse disinformation campaigns for the purposes of building legal cases. In response to deepfakes and disinformation threats like those that have emerged across the world from the 2016 United States Presidential election to Brexit in the United Kingdom and the Catalonia independence referendum in Spain, Padgett explains that 'a myriad of advanced software analytics and AI forensic tools were employed to investigate who specifically was running and sponsoring these Russian disinformation campaigns'.[70] The use of these tools to investigate Russian active measures led to the grand jury indictments against thirteen Russians and three Russian companies in February 2018.[71]

Academic institutions, military research centers and private sector entities (sometimes working in partnership) are at the forefront of the development of digital authentication technology. For example, two DARPA projects use automated tools to assess whether an image or video has been manipulated: Project Metaphor, which uses AI in media forensics, and Project Semaphore, which uses AI in semantic forensics.[72] Sophisticated digital forensic tools that can ferret out manual manipulations in digital images and videos, such as those done with Adobe Photoshop, are not as reliable when it comes to detecting AI-generated fakes. Over the last five years, in both the private and non-profit sectors, there has been an emergence of deep learning technologies to automate deepfake detection. One such company is DeepTrace, which

[69] Padgett, *supra* note 61; M. Alexander Kunz, 'Cloak: Remove Unwanted Objects in Video', Adobe Research, 11 December 2017, available online at https://research.adobe.com/news/cloak-remove-unwanted-objects-in-video/ (visited 15 January 2021).

[70] Padgett, *supra* note 61.

[71] *Ibid.*

[72] Voices from DARPA Podcast, 'Episode 33: The Verification Virtuoso', available online at https://www.darpa.mil/about-us/podcast (visited 17 February 2021)

is 'developing deep learning technologies to detect deepfakes hidden in plain sight and authenticate audiovisual media that has been manipulated'.[73] In addition, there are technology products that focus on establishing authenticity at the point of capture using a combination of hardware in mobile phones and software such as blockchain to ensure that images and videos cannot be manipulated. For example, eyeWitness to Atrocities provides a secure mobile application through which users can capture evidentiarily-sound images and videos on their mobile phones, which are directly sent to a digital evidence vault maintained by LexisNexis to ensure their chain of custody.[74] While versions of the image could still be manipulated, there will always be an unaltered original to use for comparison. Similarly, ProofMode and TruePic provide mobile applications with similar authentication technology built in from the start.[75]

In addition to technical solutions, there will always be the need to deploy human verification techniques. Reliance entirely on machines creates new problems because of 'artificial stupidity', which refers to the way algorithms can misinterpret the world in ways no human ever would, because they interpret data in terms of mathematics and logic without the overlay of instinct, intuition, or common sense.[76] The internet offers numerous websites with tips and tricks to fool facial recognition technology from hats outfitted with LED lights to makeup intended to dazzle computer vision.[77] And yet, while these ploys might outwit some algorithms, they would be quickly noticed by any human being. Another example from DARPA project manager Matt Turek is an AI-generated Airbnb listing that touted '24/7 carpeting', a semantic error that eluded machines but that most humans would catch.[78] Verification techniques such as those offered in the methodology of the *Berkeley Protocol on Digital Open Source Investigations* must be used in parallel with AI tools that assess the digital, physical, and semantic integrity of digital material.[79]

In order to establish the authenticity of physical evidence, courts look at the chain of custody from the point at which the investigator takes custody of the item until the time it is presented in court. When it comes to digital evidence, particularly online content, the challenge to authenticity comes with establishing the chain of custody from the point of creation until the time it is collected

[73] Padgett, *supra* note 61.

[74] See eyeWitness to Atrocities at https://www.eyewitness.global/welcome (visited 17 February 2021).

[75] See ProofMode at https://guardianproject.info/apps/org.witness.proofmode/ and Truepic at https://truepic.com/ (websites visited 17 February 2021).

[76] M. Trazzi and R.V. Yampolskiy, 'Artificial Stupidity: Data We Need to Make Machines Our Equals', 1 *Science Direct* (2020), available online at https://www.sciencedirect.com/science/article/pii/S2666389920300210 (visited 15 February 2021), at 1–3.

[77] For example, see E. Thomas, 'How to Hack your Face to Dodge the Rise of Facial Recognition Tech', *Wired*, 1 February 2019, available online at https://www.wired.co.uk/article/avoid-facial-recognition-software (visited 15 February 2021).

[78] Trazzi and Yampolskiy, *supra* note 76.

[79] Verification of online information falls into three main categories — content analysis, source analysis and technical analysis — and includes techniques such as reverse image search, geolocation, and chronolocation. See Berkeley Protocol, *supra* note 6.

by the investigator. If false data is generated and distributed for strategic reasons during an armed conflict, any data about that conflict could be thrown into question. Thus, there will almost always be a need for human testimony to introduce the data to lay the foundation for its authenticity and reliability. While some might assume that digital evidence could one day replace the need for witness testimony, quite the opposite is true since it will be digital evidence that often needs to be introduced at trial through human testimony. Courts will want to go beyond the question of whether or not the purported evidence has been altered but will also need to know how it was used.

Key issues which will require solutions include the lack of institutional separation between the prosecution function and the investigation and operations functions of international prosecutors' offices, the lack of sufficient procedural safeguards, and the piecemeal infrastructure with interoperability challenges. The value of evidentiary hearings in the common law system is that it forces adversarial parties to challenge each other's assumptions in a public forum, not only informing the judges in order for them to determine the proper reliability and weight of the information, but also informing the public. Lawyers will need the knowledge and confidence to challenge technical aspects of digital evidence by learning to interrogate algorithms as well as expert conclusions and qualifications. NGOs supporting war crimes prosecutions in the future will need to become better informed on how to collect and handle digital evidence, and victim populations will need a better understanding of the nuances of the process. Finally, articulate and thorough judicial reasoning on evidentiary decisions regarding digital military data will serve as a critical pillar in this process.

4. Conclusion

War crimes investigations are already improving as investigators at international criminal courts and tribunals, national war crimes units, commissions of inquiry, and non-governmental organizations adopt military-born technologies in their work. Open source intelligence and digital investigation techniques are presently used by many of these entities[80]; and increasingly, image and facial recognition, predictive algorithms, and behavioural biometrics are being experimented with to both identify and analyse evidence.[81] International investigators also use specialized mobile applications to capture and authenticate digital images and videos,[82] purchase high-resolution commercial satellite imagery for geospatial analysis,[83] and even deploy drones. In the past few

[80] Dubberley, Koenig, and Murray (eds), *supra* note 43.

[81] Amnesty International, 'Amnesty Decoders', available online at https://decoders.amnesty.org (visited 17 February 2021).

[82] WITNESS, 'Video as Evidence Field Guide', available online as https://vae.witness.org/video-as-evidence-field-guide/ (visited 17 February 2021).

[83] M. Farfour, 'Remote Sensing for Documenting Human Rights Abuses', Citizen Evidence Lab, 11 December 2019, available online at https://citizenevidence.org/2019/12/11/remote-sensing-for-documenting-human-rights-abuses/ (visited 15 February 2021).

years, international criminal trials have witnessed the use of photogrammetry to replicate crime scenes in the courtroom and virtual reality to transport judges to the battlefield.[84]

The quest for military advantage is one of the greatest drivers of innovation. In 1924, technological development for military purposes focused on kinetic power, with many perceiving increasingly bigger and better bombs as the key to victory. Current trends show that technological development for military purposes will focus on data, with requirements for bigger datasets, more accurate data, and better data analysis as the key to operational success. The same technologies used to make militaries more effective in war could similarly be used in the prevention of war, humanitarian responses to war, and investigations of alleged war crimes. International criminal investigators will benefit greatly by finding applications for these new and emerging technologies in their work, but they cannot do this alone. International criminal investigators will need to form strategic partnerships with technology companies, convince states of the need to invest in innovation, and get everyone in the field thinking about how best to prepare for the impending challenges rather than reacting to them after the fact. Utilizing AI could bring tremendous benefit to international criminal investigators seeking to hold high-level perpetrators accountable for war crimes, but at the same time failing to understand these new technologies greatly risks widening the impunity gap.

Technology is not inherently good, bad, or neutral. Rather, it is the application of the technology that determines whether it will further the ends of war or peace — and ultimately, justice. There is no more clear-cut example of this truth than the use of AI, which is simultaneously deployed in modern armed conflicts to elucidate *and* to obscure facts. In order to utilize these technologies to further the aims of international criminal justice, international courts and tribunals must ensure that their workflows, infrastructure and technical skills of the staff are equipped for investigating warfare shaped by AI. This means proactively creating room for experimentation and innovation, investing money in future-thinking solutions, establishing networks and relationships to strengthen the likelihood of data sharing, and tackling solutions to problems before they arise. As the negative societal impact of deepfakes and other forms of disinformation increases, investigators must adopt aggressive tactics to establish the truth and ensure public trust in that truth. We are living in an era in which human rights defenders and international criminal investigators and prosecutors are under constant attack. They will need every weapon in their arsenal to fight back.

[84] M. Cieslak, 'Virtual reality to Aid Auschwitz War Trials of Concentration Camp Guards', BBC News, 20 November 2016, available online at https://www.bbc.com/news/technology-38026007 (visited 17 February 2021); J. Diaz, 'How VR is Helping Convict Nazis in Court', Fast Company, 10 January 2018, available online at https://www.fastcompany.com/90156138/how-vr-is-helping-convict-nazis-in-court (visited 15 February 2021).