Autonomous weapons systems and changing norms in international relations

Ingvild Bode*
Lecturer, School of Politics and International Relations, University of Kent

Hendrik Huelss**
Postdoctoral Researcher, School of Politics and International Relations, University of Kent

Abstract

Autonomous weapons systems (AWS) are emerging as key technologies of future warfare. So far, academic debate concentrates on the legal-ethical implications of AWS but these do not capture how AWS may shape norms through defining diverging standards of appropriateness in practice. In discussing AWS, the article formulates two critiques on constructivist models of norm emergence: first, constructivist approaches privilege the deliberative over the practical emergence of norms; and second, they overemphasise fundamental norms rather than also accounting for procedural norms, which we introduce in this article. Elaborating on these critiques allows us to respond to a significant gap in research: we examine how standards of procedural appropriateness emerging in the development and usage of AWS often contradict fundamental norms and public legitimacy expectations. Normative content may therefore be shaped procedurally, challenging conventional understandings of how norms are constructed and considered as relevant in International Relations. In this, we outline the contours of a research programme on the relationship of norms and AWS, arguing that AWS can have fundamental normative consequences by setting novel standards of appropriate action in international security policy.

Keywords

Autonomous Weapons Systems; Norms; Constructivism; Practices

Introduction

There is a danger that time is running out – is debate and development of policy even still possible, or is the technological genie already out of the ethical bottle, embarking us all on an incremental and involuntary journey towards a Terminator-like reality.¹

In the shadow of drone warfare, the autonomy of weapons systems is accelerating largely outside of public and academic attention in the discipline of International Relations (IR).² The US Department
of Defense’s ‘Unmanned Systems Integrated Roadmap 2013–2038’ sets out a concrete plan to
develop and deploy weapons with ever-increasing autonomy in the air, on land, and at sea in the
next twenty years. A defining feature of these autonomous weapons systems (AWS) is precisely their
ability to operate autonomously: ‘robotic weapons …, once activated, can select and engage targets
without further human intervention’.3

Most modern weapons systems are computer-assisted and the tasks assigned to these programmes
are ever increasing. Yet the autonomous quality of weapons systems typically refers to their ability to
‘think’ and ‘make decisions’ in the broad, technical sense. This ability is the basis for searching and
identifying targets within a set of preprogrammed parameters based on sensor input. While AWS
currently in development or use are comparatively ‘stupid from an AI [artificial intelligence] per-
spective’, fast-moving advances in AI research are very likely to filter into weapons systems.4 The
robotics industry, supported by states such as the US, the UK, China, South Korea, and Russia,
therefore continues developing dual-use technology and more autonomous weapons systems,
meaning that their deployment could become a practical fait accompli in the near future. Not-
withstanding their future level of technological sophistication, ‘stupid’ autonomous weapons systems
clearly require (analytical) attention now.5

In principle, a dense network of domestic and international structures, both legal and normative,
governs the use of such security instruments. These legal structures provide standards of how and
when the deployment of different types of weapons is lawful. International law, enshrined in the
United Nations (UN) Charter and various treaties of international humanitarian and human rights
law, sets rules for what kinds of weapons are prohibited (for example, nuclear, biological, and
chemical weapons, cluster bombs), when the use of force is legal, and how weapons ought to be used.
The normative structure comprises domestic and internationally accepted norms, understood as
standards of appropriateness in this article, as well as values and ethical concerns, including the
question of what is ‘right’ and ‘wrong’ in warfare.6

and international law: Preventive security governance’, European Journal of International Security, 1:1
(27 February 2016), pp. 94–111; Michael Carl Haas and Sophie-Charlotte Fischer, ‘The evolution of targeted
killing practices: Autonomous weapons, future conflict, and the international order’, Contemporary Security

3 Christof Heyns, ‘Autonomous weapons systems: Living a dignified life and dying a dignified death’, in Nehal
Bhuta et al. (eds), Autonomous Weapons Systems: Law, Ethics, Policy (Cambridge: Cambridge University
Post blog (16 January 2015), available at: [http://www.huffingtonpost.com/heather-roff/autonomous-or-
semi-autono_b_6487268.html].
5 Ingvild Bode and Hendrik Huelss, ‘Why “Stupid” Machines Matter: Autonomous Weapons and Shifting
Norms’, Bulletin of the Atomic Scientists (12 October 2017), available at: [https://thebulletin.org/why-
“stupid”-machines-matter-autonomous-weapons-and-shifting-norms11189]; Toby Walsh, ‘Elon Musk Is
Wrong: The AI Singularity Won’t Kill Us All’, Wired (20 September 2017), available at: [http://www.wired.co.
uk/article/elon-musk-artificial-intelligence-scaremongering].
6 Alex Leveringhaus, Ethics and Autonomous Weapons (London: Palgrave Macmillan, 2016); William M.
Fleischman, ‘Just say “no!” to lethal autonomous robotic weapons’, Journal of Information,
pp. 211–27.
In theoretical terms, law and norms co-constitute each other but are not identical. This point is largely neglected by research that prioritises the regulative qualities of constitutional norms, focusing on whether state practices comply with legal standards that are equated with norms in IR. The academic debate on AWS illustrates this conventional focus: the deployment and emergence of weapons systems is assessed against existing legal standards and further options for regulation are sounded. However, the literature fails to consider that practices related to the development, testing, training, or usage of AWS outpace public, governmental, and legal considerations. As we argue, AWS may shape norms in practice by privileging procedural norms that are detached from deliberative processes. We get to this process by asking: what are the implications of developing and deploying AWS for international norms?

In answering this question, we criticise constructivist norm-emergence models via practice theories in two ways. First, we suggest that norms do not only emerge in deliberative processes, but also in practices. Models of norm emergence and change associated with both the second (late 1990s) and the third (mid-2000s) waves of constructivism focus almost exclusively on deliberative processes: norms are the outcome of open, public debate. Constructivist scholars have examined how technologies such as nuclear weapons have eventually triggered the creation of new, fundamental norms after lengthy processes of deliberation and negotiation. In contrast, we are interested in how norms and associated normative content may emerge in practices, understood as patterned actions in social context. In our case, these are practices of developing, training, testing, and deploying autonomous weapons systems and changing norms.

---

autonomous weapons systems. In accentuating the constitutive quality of practices as sites of norm emergence and change, we depart from the focus on the regulative qualities of norms prevalent in studies of AWS. Focusing on practices surrounding AWS therefore goes beyond examining how they are governed by norms towards how they create, shape, and define norms.

Second, studying practices necessitates broadening our understanding of which norms are relevant in International Relations. Constructivist research has concentrated on ‘fundamental norms’ such as human rights or non-proliferation, defining standards of legal-public appropriateness. But a different type of norm may emerge in practices: procedural norms defined as standards of procedural-organisational appropriateness, such as efficiency. The difference between fundamental and procedural norms amounts to whether promoted actions are morally right or functionally suitable. Examining practices around AWS can therefore capture an analytically interesting interplay of procedural and fundamental norms. In this process, procedural norms may affect the content of fundamental norms by either filling them with diverging substance or by pushing forward novel standards of appropriateness that might become dominant as the ‘right’ way of doing things.

In arguing these points, the contribution of this article is threefold: first, it outlines the contours of a new research agenda on the relationship of norms and AWS. Second, it establishes critical connections between practice theories and constructivist research on norm emergence. Third, in conceptualising how AWS may create and challenge norms, it also contributes to the debate on whether they should be pre-emptively banned. Regardless of the difficulties associated with finding an international, deliberative consensus on defining autonomy, this article shows that the current multitude of practices in developing, testing, and using AWS creates de facto standards of what counts as appropriate. As this happens outside the public purview, it should be very closely monitored – in particular as it may make the process of agreeing on new binding legal regulation more challenging.

The remainder of the article is structured as follows: a first section presents an overview of the development and deployment of AWS. This justifies why AWS should be examined at this point in time and prepares the ground for analysing the emergence of norms in practices. A second section outlines the current state of research on AWS and its implications for what we aim to achieve. In a third section, we cover our theoretical model on how procedural norms may emerge in practice in more detail. A fourth section discusses how AWS could influence an understanding of procedural-organisational appropriateness that diffuses to the legal-public dimension. We conclude that AWS

15 Wiener, ‘Contested compliance’.
17 As the autonomy of weapons systems evolves along a trajectory encompassing remote-controlled systems such as drones, the article recurs on these instruments to illustrate the impact of emerging standards of appropriateness.
can have fundamental normative consequences by setting novel standards of appropriate action in international relations and international security policy.

**The emergence of autonomous security technologies**

The defining aspect of AWS is their varying degree of autonomy – ultimately, independent ‘agency’. On a spectrum comprising a simple reactive mechanism at one end and human intelligence at the other end, AWS are gradually moving towards the latter. In this sense, AWS are defined as ‘systems that, once activated, can track, identify and attack targets with violent force without further human intervention’. Hence, AWS qualitatively surpass remote-controlled systems, such as drones, that are currently important security technologies.

How to define the autonomy of weapons systems is a matter of debate in two main ways. First, some scholars refine the conceptual understanding of autonomy by, for example, outlining its characteristic aspects such as independence, cognitive skills, and cognitive architecture. Heather Roff connects autonomy directly to four functions of weapons systems (trigger, targeting, navigation, mobility), allowing her to evaluate the extent to which weapons operate autonomously to different degrees. In discussing autonomy, scholars emphasise that it should not be equated with human intelligence or ‘free will’, given the distinct nature of robot decision-making. A second group of scholars debates levels of appropriate human supervisory control, focusing on human-machine interaction and the extent to which machine autonomy undermines human autonomy. Here, scholarship worries about the human role moving further and further away from immediate decision-making processes on the use of force, a concern underlined by the prominent image of the control ‘loop’. While humans are still ‘in the loop’, in manual control, with regard to drones, in the context of more autonomous systems, humans are projected to first become ‘on the loop’, only overseeing operations and having the formal ability to override machine’s decision, to eventually ‘out of the loop’, being completely absent from operating systems. The control loop image has been criticised for offering ‘a crude distinction’, because decision-making can be both immediate, that is, in an individual targeting situation, or a wider concept, that is, associated with programming.

However, where decisions are taking place may be less decisive than what kind of control will be exercised. Humans will most likely keep elements of control and oversight in future targeting decisions of AWS, but will this control be formal rather than meaningful? Even meaningful human

---

21 Roff, ‘Autonomous or “Semi” Autonomous Weapons?’.
control, a concept that has gained currency in the debate on AWS, can indicate very different things. Noel Sharkey’s five levels of human supervisory control, for example, range from humans deliberating about specific targets before initiating an attack, via humans choosing from a list of targets suggested by a program, to programs selecting targets and allocating humans a time-restricted veto. The content of meaningful human control as well as the extent to which human decision-making will be replaced or pushed back to the programming stage is debatable and will arguably emerge in practice.

While we do not aim at predicting in what ways AWS will operate in the future and how human-machine interaction will be designed, we maintain that AWS represent qualitatively different weapons systems characterised by the emergence of non-human agency. To quote former UN Special Rapporteur Christof Heyns, a key agenda-setter for the topic at the UN:

> their [AWS] deployment would entail not merely an upgrade of the kinds of weapons used, but also a change in the identity of those who use them. With the contemplation of LARs [lethal autonomous robotics], the distinction between weapons and warriors risks becoming blurred, as the former would take autonomous decisions about their own use.

The most controversial issue is the possibility that machines may make and execute the decision to end human life autonomously with severe effects on human dignity, a human right at the heart of contemporary international legal architecture. This is a crucial, qualitatively different feature of AWS in comparison to drones, for instance. Pressure to remove human decision-making in an immediate sense from target engagement and selection will potentially increase as the speed to which AWS are able to process information and execute actions autonomously grows and begins to represent an operational advantage, compared to the ‘slow’ response time of humans.

The deployment of AWS is not a scenario for the distant future. AWS are currently developed, tested, and deployed by the United States, China, Israel, South Korea, and Russia, to name some key actors. Since 2013, the international community is discussing AWS under the framework of the UN Convention on Certain Conventional Weapons (CCW). State parties to the CCW have held three informal meetings of experts since 2014. After little initial progress, the state parties agreed to formalise deliberations on AWS by creating a Group of Governmental Experts (GGE) in December 2016. While the GGE only has a discussion mandate, similar mechanisms have in the past eventually led to regulation agreements. Chaired by India, the Group has met for the first time in mid-November 2017, witnessing growing support among the CCW contracting parties for a ‘legally-binding instrument on fully autonomous weapons’. As of November 2017, 22 countries called for

30 For a more detailed discussion, see section entitled ‘AWS and procedural norms’.
a pre-emptive legal ban on AWS, a group that does not include any of the major actors developing such technologies. During the CCW’s fifth Review Conference in 2016, China released its first position on AWS, declaring that ‘China supports the development of a legally binding protocol on issues related to the use of AWS, similar to the Protocol on Blinding Laser Weapons, to fill the legal gap in this regard.’ The reference to this Protocol is interesting as it instituted a pre-emptive ban. At the same time, China has not defined AWS, making it difficult to assess the specificity of its position.

This is characteristic of discussions at the CCW, which are hampered by diverging viewpoints on autonomy and the resulting lack of a conceptual consensus on AWS. While some member states lack even a working definition, those put forward by, for example, the US and the UK differ significantly. The US defines an AWS as ‘a weapon that, once activated, can select and engage targets without further intervention by a human operator’ in Department of Defense (DoD) Directive 3000.09 that will be discussed further below. The Directive also includes a contested distinction between so-called semi-autonomous and autonomous weapons: semi-autonomous weapons can ‘employ autonomy’ for a full range of ‘engagement-related functions’ for ‘individual targets or specific target groups that have been selected by a human operator’. The utility of this distinction is contested as target selection, under-defined in the Directive, becomes the only marker to distinguish semi-autonomous from autonomous weapons systems, making it ‘a distinction without difference’.

The UK differentiates between an ‘automated’ and an ‘autonomous system’: ‘an automated or automatic system is one that, in response to inputs from one or more sensors, is programmed to logically follow a predefined set of rules in order to provide an outcome. Knowing the set of rules under which it is operating means that its output is predictable.’ In contrast, an autonomous system is defined as capable of understanding higher-level intent and direction. From this understanding and its perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control, although these may still be present. Although the overall activity of an autonomous unmanned aircraft will be predictable, individual actions may not be.

This definition of autonomous systems departs distinctly from an earlier UK definition in including the qualifiers ‘higher-level intent and direction’, thereby arguably ‘defining away’ the challenges associated with short-term AWS.

---

33. The group calling for a ban comprises (November 2017): Algeria, Argentina, Bolivia, Brazil, Chile, Costa Rica, Cuba, Ecuador, Egypt, Ghana, Guatemala, Holy See, Iraq, Mexico, Nicaragua, Pakistan, Panama, Peru, State of Palestine, Uganda, Venezuela, and Zimbabwe.


38. Roff, ‘Autonomous or “Semi” Autonomous Weapons?’.


40. Ibid., p. 72.

Domestically, the US Directive 3000.09 ‘lays out guidelines for the development and use of autonomous and semi-autonomous weapon systems’.\textsuperscript{42} The Campaign to Stop Killer Robots, an international NGO coalition advocating for a pre-emptive ban, has welcomed Directive 3000.09 because it represents the first national policy on AWS.\textsuperscript{43} Human Rights Watch has even characterised the policy as ‘the world’s first moratorium on lethal fully autonomous weapons’ due to its attached ten-year expiration date and the restrictions on what it defines as AWS to use lethal force.\textsuperscript{44}

However, as Mark Gubrud points out, this is a misreading:\textsuperscript{45} first, with reference to a DoD spokesperson, ‘the 10-year expiration date is routine for such directives’ rather than representing a moratorium.\textsuperscript{46} Second, Directive 3000.09 also outlines ways of waiving even the restrictions it places on the lethal use of AWS.\textsuperscript{47} It further explicitly notes that widely defined ‘semi-autonomous weapon systems … may be used to apply lethal or non-lethal, kinetic or non-kinetic force’.\textsuperscript{48} Therefore, Directive 3000.09 ‘signals to developers and vendors that the Pentagon is serious about AWS’.\textsuperscript{49} Further, codifying that ‘[a]utonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force’ will be ‘ineffective and irrelevant’ with regard to technological advances and operational demands potentially leading to the emergence of fully autonomous weapons systems.\textsuperscript{50}

Considering the various research programmes, initiatives, and tests that show to what extent AWS are developed, tested, and already in use, it becomes clear that the emergence of legal regulations lags behind, which increases the importance of moving beyond a legal perspective and considering how norms may emerge in practice.

\textbf{AWS in action}

Although fully autonomous weapons systems, that is, systems with independent target selection, are not yet operational, their research and development is constantly proceeding. AWS can take many different forms, from singular entities to swarms, and they can operate on land, in air, and at sea. Many existing weapons platforms are arguably only a software update away from increasing autonomy. To give a few examples of current systems, in December 2016, the US Office of Naval research released a statement that autonomous unmanned swarming boats successfully performed a testing exercise, noting that unmanned boats were given a large area of open water to patrol. As an unknown vessel entered the area, the group of swarmboats collaboratively determined which patrol boat

\textsuperscript{43} Campaign to Stop Killer Robots, ‘New US Policy’ (16 April 2013), available at: [https://www.stopkillerrobots.org/2013/04/new-us-policy/].
\textsuperscript{44} Human Rights Watch, ‘Review of the 2012 US Policy on Autonomy in Weapons Systems’.
\textsuperscript{45} We thank an anonymous reviewer for drawing our attention to this point.
\textsuperscript{47} Gubrud, ‘Semi-Autonomous and on Their Own’.
\textsuperscript{49} Gubrud, ‘US Killer Robot Policy’.
\textsuperscript{50} Dan Saxon, ‘A human touch: Autonomous weapons, DoD Directive 3000.09 and the interpretation of “appropriate levels of human judgment over the use of force”’, in Bhuta et al. (eds), \textit{Autonomous Weapons Systems}, p. 183.
would quickly approach the unknown vessel, classify it as harmless or suspicious, and communicate with other swarmboats to assist in tracking and trailing the unknown vessel while others continued to patrol the area.51

In January 2017, the US DoD announced the successful test of a large micro-drone swarm in air, consisting of 103 ‘Perdix’ drones: ‘[t]he micro-drones demonstrated advanced swarm behaviors such as collective decision-making, adaptive formation flying, and self-healing.’52 In this context, then US Secretary of Defense Ash Carter remarked that ‘[t]his is the kind of cutting-edge innovation that will keep us a step ahead of our adversaries. This demonstration will advance our development of autonomous systems.’53 These examples demonstrate that swarms of ‘smaller and smarter … systems would be able to make decisions and coordinate themselves without constant human supervision – perhaps without any contact at all.’54

While the above systems are so far mainly designed for defensive, surveillance, or reconnaissance purposes, developments also move towards offensive systems. The US Navy is further developing a submarine-hunting drone ship, the Sea Hunter, which has become operational in late 2016. While the Sea Hunter is still remotely controlled,

the progress of the platform’s technology, and the rapid advancements of algorithms enabling greater levels of autonomy, have inspired the Navy to begin thinking about additional missions … so that it can conduct surface warfare missions, fire weapons and launch electronic attacks.55

Developments are not confined to the US. In the 2000s, Israel has developed the Israel Aerospace Industries (IAI) HAROP, a loitering munition that has so far been operated by Israel, India, and Azerbaijan. The IAI note that ‘HAROP searches, finds, identifies, attacks and destroys targets, and performs battle damage assessment’ as an ‘autonomous platform operation’.56 HAROP is therefore able to engage targets autonomously and to destroy them via a self-destructing attack. According to media sources, Azerbaijan used HAROP for a deadly attack on a bus during the Nagorno-Karabakh conflict in April 2016.57

These examples also point to an important, shared characteristic of these weapons systems: they have different modes of operation, enabling switching between different modes at the interstice of

53 Ibid.
automation and autonomy. South Korea’s SGR-A1, a stationary sentry robot developed in the 2000s that has been used at the Korean Demilitarized Zone, illustrates this observation. As it is equipped with heat and motion sensors and an auto-firing system,\(^5\) the system can theoretically detect, select, and engage a human target without human intervention. However, to what extent the SGR-A1 could be easily switched to and operated at an autonomous mode remains unclear. Table 1 provides an overview of some current weapons systems that operate without direct human intervention.\(^5\)

### Researching AWS: Questions of law and ethics

So far, research has explored AWS alongside two main, often interconnected lines: their (potential) legality and ethical challenges attached to their usage. We summarise these studies first before commenting on gaps in this literature.

First, studies of legality examine the extent to which AWS can or could potentially comply with international (humanitarian and human rights) law. General *jus in bello* principles governing the use of force, such as distinction, proportionality, and accountability, raise important concerns regarding the implications of increasing autonomy for complex aspects. Scholarly opinion about proportionality differs: while some regard AWS as potentially more precise weapons decreasing human suffering,\(^6\) as underlined by the benefits of ‘precision-guided homing munitions such as torpedoes’,\(^6\) others argue that AWS increase the recourse to violent instruments, affecting proportionality negatively and making escalations more likely.\(^6\) A decision about the proportional use of force

<table>
<thead>
<tr>
<th>Missile and rocket defence systems</th>
<th>Goalkeeper close-in weapon system (Netherlands)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Iron Dome (Israel)</td>
</tr>
<tr>
<td></td>
<td>Kashtan close-in weapon system (Russia)</td>
</tr>
<tr>
<td>Anti-personnel sentry weapons</td>
<td>Samsung SGR-A1 (Republic of Korea)</td>
</tr>
<tr>
<td></td>
<td>Guardium (Israel)</td>
</tr>
<tr>
<td></td>
<td>MDARS-E (USA)</td>
</tr>
<tr>
<td>Loitering munitions</td>
<td>Harpy, Harop (Israel)</td>
</tr>
<tr>
<td>Combat air vehicle (aircraft carrier-based)</td>
<td>Northrop Grumman X-47B (USA)</td>
</tr>
<tr>
<td>Surface vehicle</td>
<td><em>Sea Hunter</em> (US)</td>
</tr>
<tr>
<td></td>
<td>Protector USV (Israel)</td>
</tr>
<tr>
<td></td>
<td>Silver Marlin (Israel)</td>
</tr>
<tr>
<td>Combat ground vehicle</td>
<td>Uran-9 (Russia)</td>
</tr>
<tr>
<td></td>
<td>MRK-27 BT (Russia)</td>
</tr>
</tbody>
</table>

---


requires assessing and processing complex data that might be based on contradictory signals if measured against a preprogrammed set of criteria-action sequences characteristic of autonomous ‘decision-making’. Critics of AWS also point to their inability of meeting requirements of distinction – that is differentiating between civilians and combatants and therefore unlawful and lawful targets in complex environments.\(^6^3\) Whether a vehicle is used for combat purposes or not, whether an armed individual is a fighter or a civilian, or whether a group comprising some armed individuals also comprises civilians, are questions of human judgement requiring highly complex reflection processes that pose fundamental challenges for deploying AWS.\(^6^4\)

With regard to accountability, legitimacy is often linked to public demands of individual and political responsibility when force is used, particularly in cases that challenge norms of humanitarian law.\(^6^5\) The increasing autonomy of weapons systems raises the question to what extent different groups of individuals, engineers and programmers, political decision-makers, or military command and operating staff, are accountable for ‘decisions’ undertaken and mistakes committed by AWS.\(^6^6\) The less specific aspect of legitimacy through political-democratic accountability concerns the involvement of democratic institutions, such as parliaments, in the control of developing and deploying AWS. The question is whether existing procedures and rules for parliamentary oversight are adequate in future scenarios of large-scale AWS deployment.

Second, ethical studies cover a range of challenges associated with the potential deployment of AWS, centering on the question whether autonomous weapons can ever \textit{legitimately} end human life.\(^6^7\) Many call for a comprehensive ban of AWS due to ethical issues and concerns for human dignity,\(^6^8\) while some emphasise the potential of AWS to contribute to a more ‘humane’ warfare as autonomous weapons would not be governed by emotions such as fear, hate, and revenge.\(^6^9\) Essentialising AWS as benevolent instruments often comes with highly futuristic scenarios distinct from near-term advances in AI and tends to neglect that even autonomous systems are only as good as the purpose or intentions they are meant to serve.

Contributions in the field are rich and growing but there are two important gaps: first, debates on the legality of AWS and ethical challenges attached to their usage both operate with a fixed, predefined understanding of what is right and appropriate. However, arguably, the defining feature of AWS is their developing and changing characteristics. In this regard, we require a theoretical perspective that accommodates the constitutive qualities of AWS as emerging technologies. We therefore present viewpoints on the flexible constitutions of appropriateness that come along with considering how AWS work through \textit{practices}.

\(^6^3\) Sparrow, ‘Robots and respect’.
\(^6^4\) Sharkey, ‘Saying “not” to lethal autonomous targeting’; Sharkey, ‘The evitability of autonomous robot warfare’.
\(^6^9\) Arkin, ‘The case for ethical autonomy in unmanned systems’.
As is the case with all developing weapons technologies, there is no specific regulation in international law regarding the use of AWS. Further, while remote-controlled weapons such as drones have been used extensively by the US, their usage also remains largely unregulated. States continue to operate drones in a grey zone of international law because drone warfare arguably violates the principles of distinction and proportionality and is not yet covered by specific legal regulations.70 Currently, the deployment of AWS remains legally permissible with the added uncertainty that their technological autonomy is unaccounted for.

The most problematic aspect of the legal perspective on AWS is their elusive character. Any type of regulation requires looking towards the future in defining technologies that are constantly evolving. In other words, the technical complexity, the dual-use character, and the variety of deployment scenarios makes it challenging to formulate legal restrictions on technological developments: ‘History works against preventive norm making. States usually react, as technological developments usually outpace political agreements to tackle future potential problems.’71

Yet, standards of appropriateness regarding the usage of AWS are already emerging. First, the increasing recourse to drones in the US’s approach to the use of force72 has led to the emergence of practices in the sense of routine ways of ‘how things are done’. These are far from meeting the requirements of customary international law: they do not indicate ‘dense’ (behavioural or verbal) state practice, nor do they exhibit opinio juris, ‘a belief that such practice is required … or allowed as a matter of law’.73 Yet, these practices create a status quo that makes it more difficult to challenge the further proliferation and usage of drones. In addition, only a very small number of states deploy or develop the most advanced (precursors to) AWS. This means that the emergence of customary law is even more restrained, despite the existence of practical precedents. The use and spread of the ‘unwilling or unable’ formula by the US as a ‘test’ to inform drone targeting decisions is a case in point.74

Accordingly, discussing this issue in the context of (customary) international law does not provide an adequate framework because it does not allow researchers to capture emerging standards of appropriateness attached to AWS. In contrast to considering how norms prevent or regulate, our article therefore studies how norms may emerge outside of deliberative forums and the framework of international law making.

Second, the widely unaccounted development of AWS has impeded deep public discourse on this issue. There has been media attention and civil society organisations or campaigns such as Article 36, the Campaign to Stop Killer Robots, or the International Committee for Robot Arms Control (ICRAC) seek to raise the issue’s profile. But the wider political discourse is not particularly concerned with the most fundamental questions and realities of AWS. Technological advances in this area are often incremental and come with a low political profile. Hence, the important role public acceptance plays in debating and creating dominant understandings of appropriateness is lacking.


Building on this role of the public, the (lacking) discussion on developing AWS should also be seen in
the context of overall lowering use of force standards when countering terrorism.75 Military efficiency and effectiveness as the main arguments for why drone warfare is appropriate have turned into a public legitimacy source.76 The promise of ‘surgical’ strikes and the protection of US troops has turned drones into the most ‘appropriate’ security instrument to counter terrorism abroad. The argument that AWS are ‘considered especially suitable for the casualty-averse risk-transfer war that democracies prefer’77 points to the important role AWS may play in democratic systems because they make the use of force appear more legitimate. In the case of drones, their broad acceptance across the military and political-public sphere marginalises their contested legal role. A poll conducted in 2013 showed that 75 per cent of American voters approved drone strikes ‘on people and other targets deemed a threat to the US’.78 The constitutive role that this security technology plays for international norms in terms of setting precedents and hence new standards of appropriate use of force is, however, completely out of sight.

To conclude, as the conventional frameworks of law/ethics have difficulties to accommodate flexibility and change for structural reasons, we demonstrated that it is necessary to consider other types of norms that are not accounted for in research on AWS. A purely regulative perspective on AWS risks losing track of current developments and their future implications, in particular their possible role in shaping standards of appropriateness and understandings of the ‘new normal’ in warfare.79

Researching the normativity of AWS

Research on law and ethics asks how AWS challenge the implementation of fundamental international norms, to what extent they are governed by these norms, and whether discussions in the CCW will lead to the formulation of new ‘fundamental norms’80 governing their usage. Constructivist research on norm emergence and change mirrors these questions in two main ways: first, it concentrates almost exclusively on fundamental norms with regulative qualities and second, it only studies how new fundamental norms emerge or are contested in processes of deliberation.

First, fundamental norms are typically conceptualised as closely linked to international law. Second-wave constructivist models were thus concerned with analysing the emergence, internalisation, and effects of

80 Wiener, ‘Enacting meaning-in-use’.
human rights as fundamental norms. In the context of disarmament, Nina Tannenwald prominently analysed the ‘development of a normative prohibition against nuclear weapons’, identified as one of the strongest, fundamental norms in International Relations. She defines a norm as ‘a shared expectation about behavior, a standard of right or wrong’, thereby linking norms to what is morally ‘right’. While this is certainly a key quality of norms, we argue for a broader understanding. Norms as standard of appropriateness can also comprise functional aspects such as efficiency and effectiveness in specific settings. A procedural norm in the military, for example, does not necessarily meet universal, public understandings of the morally ‘right’.

Second, the second and third wave of constructivist research focused on how norms emerge in processes of deliberation. In the second wave, actors, such as transnational advocacy networks or norm entrepreneurs, ‘attempt to convince a critical mass of states (norm leaders) to embrace new norms’. Third wave constructivist scholars criticise the sequential logic of these models by introducing more complexity and contestation. In stating that ‘norms are contested by default’, they argue for a diversity of normative meaning but these contestations still refer back to a deliberative expression of a shared norm, rather than its reconceptualisation in practice. Comprehensive regulation and stigmatisation of nuclear or chemical weapons only emerged after these weapons had been used in the First and Second World Wars, but the analytical focus of studies remains on public deliberations after usage rather than conceptualising in more detail how perceived ‘appropriate’ ways of using, later contested in deliberation, initially emerged in practices.

Technological advances below and beyond the ‘radar’ of international legal regulation might therefore set de facto norms before debates have unfolded. This also challenges the prevalent constructivist perspective that ‘a norm ... exists independently of the behavior that it guides or regulates’. In contrast, we argue that norms emerge in the context of practices. What kinds of new understandings of appropriateness emerge with the rise of AWS as security technologies in practice? As aforementioned, it is argued that ‘robotic weaponry will lower the psychological barriers to starting new wars’. AWS may contribute to lowering thresholds for the use of force because they

81 Finnemore and Sikkink, ‘International norm dynamics and political change’; Keck and Sikkink, Activists Beyond Borders; Risse, Ropp, and Sikkink, The Power of Human Rights; Risse, “Let’s argue!”.
86 Garcia, Small Arms and Security.
87 Antje Wiener, A Theory of Contestation (Berlin: Springer, 2014); Alan Bloomfield, ‘Norm antipreneurs and theorising resistance to normative change’, Review of International Studies, 42:2 (2016), pp. 310–33; Zimmermann, ‘Same same or different?’.
88 Wiener, ‘Contested compliance’.
do not put the lives of their operators at risk.\textsuperscript{93} A ‘logic of consequences’, weighing the tactical-strategic and operational advantages of AWS, could spill into a ‘logic of appropriateness’.\textsuperscript{94} What appears to be useful and efficient in procedural terms and in a specific organisational context could therefore become the new standard of what is normatively ‘right’ and legitimate. These often-conflicting understandings of appropriateness might converge in some cases: protecting the lives of a country’s own troops would not only be considered as efficient, but also, publicly, as normatively appropriate and hence legitimate.

Building on these insights, we define norms broadly as standards of appropriateness for specific practices, resting on an inclusive understanding of norms. Here, Antje Wiener’s distinction between ‘fundamental norms’, ‘organizing principles’, and ‘standardized procedures’ is helpful as it points to what we call \textit{procedural norms}.\textsuperscript{95} Wiener’s three types of norms are further specified based on three features: generalisation, specification, and contestation on ethical grounds (Table 2). Consequently, fundamental norms are considered as more general, less specific, and also as more contested on ethical grounds than the other types.

Despite drawing attention to different types of norms, Wiener’s typology is hierarchical and thereby still replicates the overall positive research bias towards fundamental norms in two ways. First, organizing principles and/or standardized procedures merely implement fundamental norms. We argue that it is conceptually important to consider a reverse of this sequence through analysing how standardized procedures and/or organizing principles may shape or define normativity. Second, the assumption of ‘ethical contestation’, in decreasing from fundamental norms to standardized procedures, suggests that the latter do not contain significant normative substance – an assumption we contest.

To gain an understanding of standardized procedures, what we call procedural norms, we suggest focusing on practices. We assume that these practices can construct new or different standards of appropriateness that turn into procedural norms when becoming widespread. Practices can therefore become decisive for studying both how procedural norms emerge and how these relate to fundamental norms.

Given that such procedural norms are subject to less ethical contestation and hence are also less in the public/academic focus than fundamental norms might make them even more relevant or powerful. Operating AWS is very much based on procedural norms – they are governed by an emerging

\textbf{Table 2. Typology of norms.}\textsuperscript{92}

<table>
<thead>
<tr>
<th>Type of norms</th>
<th>Generalisation</th>
<th>Specification</th>
<th>Contestation on ethical grounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fundamental norms</td>
<td>More</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Organising principles</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Standardised procedures</td>
<td>Less</td>
<td>More</td>
<td>Less</td>
</tr>
</tbody>
</table>

\textsuperscript{92} Based on Wiener, ‘Enacting meaning-in-use’, p. 184.


\textsuperscript{95} Wiener, ‘Enacting meaning-in-use’, p. 184.
established ‘way of doing things’. As mentioned previously, the US drone program shows how new standards of ‘appropriate’ warfare may emerge in international relations. These procedural norms are of high ethical, normative importance because overall, they are expected to conform to fundamental norms by implementing, respecting, or protecting them. How fundamental norms such as human rights influence practices, that is, what is procedurally legitimate as a ‘best practice’, is therefore often only defined via procedural norms, where operational standards of appropriateness are established.

A focus on procedural norms opens up a connection to practice theories, a diverse and dynamic theoretical programme in IR.96 Understood as patterned actions in social context,97 practices can act as sensitising concepts98 to study concrete empirical phenomena, such as the emergence of normative standards. Due to their micro-orientation, practice theory can cast light on how norms may emerge on the procedural level and therefore make the processes constitutive of the wider normative international order visible.

The emergence of a technical, autonomous ‘agency’ that comes with AWS adds another element of complexity to this. Theoretically motivated studies of drones already argue for the emergence of “technological agency” [that] shapes the evolving “field” of legal expertise (who counts as a legal expert and on what basis).99 The agency of AWS can significantly surpass this technological agency in not only shaping but eventually replacing human decision-making in the immediate sense of the term. In that, the problem emerging from ‘the anthropomorphic logic of technology’ that considers drones ‘as moral agents that can “act” rationally, dispassionately and – at least in principle – ethically’100 is intensified in the case of AWS. Varying degrees of autonomy and agency of machines play a significant role in constituting procedural norms that are usually expected to translate or follow preprogrammed parameters supposed to comply with fundamental norms. However, what happens when AWS define standards of procedural appropriateness as constitutive of normative meaning that do not match their programmers’ or decision-makers’ initial intentions? This is in line with general assumptions of actor-network theory and the ‘sociology of translation’,101 but the more sophisticated agency of AWS opens a new chapter in this regard. The autonomous agency of AWS can potentially ‘break’ the conventional network of human and technological agency. A deeper theoretical discussion of this matter is beyond the scope of this article. But, in the context of AWS, we must ask whether we move from the co-constitution of a human decision and its material execution, which is based on the assumed prevalence of human control, to a sequence where technologies

97 Leander, ‘Thinking tools’.
become the dominant constitutive, decision-making element. Furthermore, the absence of an ethical consciousness of machines in the human sense makes them particularly relevant for ethical contestations because their norm-setting qualities as fully autonomous actors will not be linked to human decisions, as was the case to date.

Based on this discussion, we propose studying AWS in the context of two different, but interrelated normative spheres: the legal-public sphere – the primary realm of fundamental norms; and the procedural-organisational sphere – the primary realm of procedural norms. While these spheres are not independent from each other, we use them to examine a broader notion of appropriateness: (1) legal-public appropriateness, and (2) procedural-organisational appropriateness.

Legal-public appropriateness represents fundamental norms, including public expectations in terms of (political) accountability, lawfulness, or transparency. In contrast, procedural-organisational appropriateness represents procedural norms, considerations of appropriateness in specific organisational settings, such as the armed forces, or in specific situations of warfare. Here, appropriateness is concerned with functional legitimacy, specific regulations, and accountability hierarchies, such as a chain of command. In this sense, appropriateness is linked to following clear procedural structures regardless of their content. In representing different contexts of appropriateness, this model accounts for diverging, interplaying layers of appropriate actions. A comprehensive research framework on the normativity of AWS should therefore consider both legal-public and procedural-organisational appropriateness (Table 3).

In sum, the category of legal-public appropriateness comprises fundamental norms such as human rights, international legal standards (international humanitarian and human rights law, *jus ad bellum* standards of the UN Charter), principles such as the pacific settlement of disputes and non-intervention, but also legitimacy expectations of the public in terms of political accountability and responsible conduct. This category hence combines legality with legitimacy. Procedural-organisational appropriateness comprises procedural norms relevant for specific organisational settings and practices. These are procedural efficiency, effectiveness, or standards in the military context such as obedience to orders, survival, or defeating the enemy. Table 3 provides examples of norms that might be relevant when studying AWS – however, it is important to emphasise that neither fundamental nor procedural norms are fixed in content. The precise importance of specific norms is only perceivable when analysing practices. In the following section, we consider how different types of appropriateness interrelate in the context of AWS and may lead to the emergence of new normativity.

### Table 3. Normative categories and examples of substance.

<table>
<thead>
<tr>
<th>Category</th>
<th>Substance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal-public appropriateness</td>
<td>Fundamental norms, e.g. human rights, democratic principles (accountability, transparency, rule of law), responsibility, protection, restrictions to use of force (<em>jus ad bellum</em> and <em>jus in bello</em>), peaceful conflict resolution</td>
</tr>
<tr>
<td>Procedural-organisational</td>
<td>Procedural norms, e.g. efficiency, effectiveness, discipline, obedience, orders, survival, strategy and tactics, deterrence, fighting the ‘enemy’</td>
</tr>
</tbody>
</table>

AWS and procedural norms

Research on AWS provides rich summaries of how their development relates to fundamental norms of legal-public appropriateness (see earlier section on this). Yet norms of procedural-operational
appropriateness are constituted by conflicting factors. Procedural norms may emerge around perceived operational advantages associated with practices surrounding AWS.

A main perceived advantage of granting full autonomy to AWS lies in their ‘superior’ ability to process a large quantity of information in contrast to humans who run the risk of facing a ‘potential cognitive overload’.102 Furthermore, AWS would have the operational advantage of having agency ‘on the battlefield’, while remote-controlled weapons are steered from a remotely positioned ‘decision-making human’. AWS could therefore collect relevant information much more comprehensively but face a double interaction problem if not used in a fully autonomous mode, that is, with the human out of the immediate decision-making loop. If functioning with a human ‘on the loop’, involved in decision-making in an immediate sense, information that is collected and processed is then transmitted to a human actor. This actor must make a decision and communicate it back to the AWS that executes the command. Both remotely-controlled weapons systems and AWS with a human ‘on the loop’ therefore normally operate at a much lower speed than fighter jets for instance. This makes them vulnerable to countermeasures, while their communication link is also susceptible to interference.103 Having a human involved therefore may be perceived to slow down the process not only by separating the decision-making and executing actors, but also by technological restrictions in terms of transmission speed.

As Thomas K. Adams notes:

Humans may retain symbolic authority, but automated systems move too fast and the factors involved are too complex for real human comprehension. When computers are designed and programmed by other computers, the situation will be even further from anything that humans can reasonably expect to understand, much less intervene in successfully.104

Not only do we have to question the quality of meaningful human control of humans ‘on the loop’ in this context, but we should also note the pressure towards giving AWS more decision-making agency due to reasons of efficiency and perceived military advantage. As Denise Garcia puts it: ‘The USA is pursuing killer robots because it can.’105 In other words, norms of procedural-organisational appropriateness set demands for not falling behind possible adversaries and allies alike, as highlighted by the UK’s Ministry of Defence: ‘Our conceptual thinking lags behind the art of the currently possible, never mind what lies in the future.’106 This increases the pressure towards proceeding with research and developing AWS ahead of any legal or political-legitimacy considerations.

Scholars have also cited budget pressures as operational advantages for AWS:107 while they require investing considerable financial resources from development to testing and training, they are projected to turn out cheaper than humans in the long run. This may become a future push factor, considering that, for example, the US Department of Veteran Affairs alone has spent an estimated US

$213 billion in medical and disability payments during the ‘War on Terror’ (2001–16) and is expected to spend another US $1 trillion until 2053.108

Further, if the argument were validated that using AWS could decrease civilian casualties compared to the status quo, they would be perceived as procedurally, organisationally, and legally appropriate. It still remains questionable whether the public would accept AWS deciding about life and death as legitimate. Initial research on public opinion shows that support for AWS differs but may be affected when it comes to protecting the life of own troops and countering the risk of foreign powers developing AWS.109 Clearly, we should also consider what kind of normativity emerges here. Although the deadly use of force by AWS is not yet a pervasive reality, the way AWS kill is constructed by some as a norm of ‘humane’ future warfare. We can easily imagine how this implicit definition of appropriateness diffuses from the procedural-organisational to the legal-public dimension.

It could be argued at this point that the norm-setting qualities of AWS are strictly limited because they are designed to execute programmed commands within a narrowly defined operational range. In this sense, the autonomous agency of machines will never equate human consciousness and awareness, typically used as a maximum definition of autonomy by states. However, the phenomenon of agency through emergent behaviour, as noted by AI scholars, questions this assumption. It refers to behaviour that is not programmed but arises out of complexity.110 This is also related to the potential misinterpretation of human signals by AWS, both in terms of the person ‘on the loop’ and those that the machine encounters in operational scenarios:

Programs with millions of lines of code are written by teams of programmers, none of whom knows the entire program; hence, no individual can predict the effect of a given command with absolute certainty, since portions of large programs may interact in unexpected, untested ways.111

This means that the actions of AWS are unpredictable to a certain extent in unstructured, complex environments and decision situations such as battlefields, a point also highlighted by Noel Sharkey: discussing various AWS under development, he notes that all work with ‘clean’ scenarios, that is, scenarios containing only military targets and no civilian populations, which is far from many real life situations.112

We should also note that AWS come with operational disadvantages in procedural terms. As an organisation and albeit not a monolith, the military is structured around control, which makes the idea of ceding it to AWS highly contested. The history of developing AWS in the US military, for example, includes various programs that were cancelled despite considerable investment113 and even

112 Sharkey, ‘The evitability of autonomous robot warfare’; Sharkey, ‘Saying “no!” to lethal autonomous targeting’.
lead to identifying ‘a cultural disinclination to turn attack decisions over to software algorithms’.\textsuperscript{114} The targeting software included in AWS exceeds human capacities in processing large datasets and other quantitative tasks, but they are disadvantaged compared to humans when it comes to deliberative reasoning, interpreting qualitative data, or accurately judging complex social situations and interactions.\textsuperscript{115} For example, in identifying targets, AWS would be unable to make qualified judgements based on interpreting facial expressions or body language in the same way humans can. Judging situations also concerns crucial assessments, such as whether an armed attack has occurred. This can be underlined by a famous 1983 incident involving Stanislav Petrov, a Soviet officer who disregarded an incoming nuclear missile strike, actually wrongly identified by the early-warning system, as a false alarm, deciding not to report it to superiors who would have retaliated with a nuclear attack.\textsuperscript{116} An autonomous system working within preprogrammed parameters would have not been able to ‘feel’ that something was suspicious about incoming data points.

Therefore, there are also procedural norms working against AWS on an operational level. Yet we consider that the current development and deployment trajectories point towards AWS with disastrous consequences for use of force thresholds. Further, once introduced by one actor, their (future perceived) procedural advantages will shape new norms of procedural appropriateness, putting pressure on other actors to follow suit.

**Conclusion: the normative consequences of AWS**

This article addressed the emergence of procedural norms through evolving AWS and resulting challenges to constructivist approaches in IR. It outlined that fundamental norms enshrined in international law are expected to govern the usage of AWS in the same way as other technologies of warfare. But can technologies such as AWS be simply regulated by a set of predefined rules or do standards of appropriateness also emerge in practices? In addressing this question, we criticised first, how constructivist approaches privilege the deliberative over the practical emergence of norms and second, how they overemphasise fundamental norms to the detriment of procedural norms. We argue that procedural norms emanating from practices play an un-examined role in emerging normative structures. Instead of merely focusing on how norms regulate or govern AWS, we therefore suggest reversing the perspective and considering how AWS may construct and define norms in practice. In this, we map out a new programme for research both for constructivist scholars interested in norm emergence and scholars of AWS.

Existing research on AWS asks some central questions: can or do AWS conform to international law? How do AWS affect fundamental norms embedded in international law, such as human rights? How do autonomous technologies relate to expectations of political accountability and responsibility? Should AWS be pre-emptively banned? But research neglects that normativity may already emerge from their development, testing and deployment on the procedural, practical level. How AWS may set novel understandings of appropriate action remains understudied. To capture this dynamic analytically, our theoretical approach differentiates between two sets of norms: fundamental norms that define legal-public appropriateness and procedural norms that define procedural-organisational appropriateness.


\textsuperscript{115} Heyns, ‘A/HRC/23/47’; Sharkey, ‘Staying in the loop’.

\textsuperscript{116} Paul Aksenov, ‘Stanislav Petrov: the man who may have saved the world’, *BBC Russian* (26 September 2013), available at: [http://www.bbc.co.uk/news/world-europe-24280831].
This understanding stands in contrast to the primary focus on fundamental norms present in constructivist norms research. We argue that understandings of what is procedurally appropriate in a specific organisational environment are often in conflict with expectations of legal-public appropriateness.

This is an important change of perspective as neither specialised literature on AWS, international/domestic law, nor constructivist research on norms has yet developed a substantial normative foundation for assessing the implications of AWS. As a normative consequence of this gap, current practices surrounding the development and usage of AWS effectively define ‘normal’ action in international relations. A similar development is already underway in the deployment and proliferation of drones as major instruments of contemporary counterterrorism. The US drone program has set novel precedents for how ending human life is ‘appropriate’ – not because these practices specifically comply with international law or adhere to domestic norms, but because they satisfy procedural-organisational appropriateness and partly coincide with publicly accepted legitimacy of the ‘War on Terror’. It will be difficult to return to a status quo before this new normality was created because other actors can now potentially exploit this room of maneuver at their discretion.

In this regard, the problem of agreeing on a general, pre-emptive ban of AWS lies in their elusiveness. Scholars continue to debate definitions of autonomy, agency, technical features, operational aspects, and appropriate human supervisory control in the context of AWS. Finding state-based consensus for a definition of AWS at the CCW that could become the basis for negotiating a regulative legal framework proves to hamper the process. Regardless of whether a ban will or will not be imposed, the practice of AWS will already shape understandings of what is appropriate and thereby take the place of a more profound societal-political debate on what is normatively acceptable. We need to be aware of these normative consequences of AWS in order to assess the role they will play in future security policies and international relations in general.

Acknowledgements

The authors would like to thank the members of the Conflict Analysis Research Centre at the University of Kent, participants at the 2017 annual convention of the International Studies Association, as well as two anonymous reviewers for their helpful comments.

Biographical information

Ingvild Bode is Lecturer in International Relations at the University of Kent. She is currently a member of the Board of Directors of the Academic Council on the United Nations System. Her research focuses on processes of normative change in international peace and security at the United Nations, with a theoretical focus on practice theories. She is particularly interested in changing standards on the use of force. Her most recent book is *Individual Agency and Policy Change: The People of the United Nations* (Routledge). She has also published in leading international journals such as the *European Journal of International Relations*, *International Studies Perspectives*, and *Global Governance*.

Hendrik Huelss is a Postdoctoral Researcher in the School of Politics and International Relations, University of Kent. His main research interests are in the broad theme of human-technology relations in the contexts of European Studies and International Relations. His primary theoretical research is on the concept of governmentality. Currently, he investigates the implications of autonomous weapons systems, the EU’s external relations with a focus on women’s empowerment, and norms in IR, emphasising the role of technologies.