LE IMPLICAZIONI ETICO-GIURIDICHE DELLE NUOVE TECNOLOGIE ROBOTICHE ED INFORMATICHE IN CAMPO MILITARE TRA *LEX LATA* E *LEX FERENDA*

Daniele AMOROSO

(Università degli Studi di Cagliari)

e

Guglielmo TAMBURRINI

(Università degli Studi di Napoli Federico II)

1. Introduzione

In uno scritto pubblicato sul finire dello scorso millennio, Cristopher Greenwood elogiava la capacità dei principi internazionali sulla disciplina degli armamenti di affrontare le sfide poste dallo sviluppo di nuove tecnologie militari e fissava, come priorità per il secolo a venire, non già l'adozione di nuove norme (*lex ferenda*), quanto piuttosto l'effettiva applicazione dei quelle vigenti (*lex lata*).[1] Questo breve contributo intende verificare la correttezza di questo assunto alla luce dei recenti tentativi della comunità internazionale di dare una risposta alle questioni etico-giuridiche poste da tre tecnologie che stanno rivoluzionando il modo di fare e concepire la guerra (o promettono di farlo nel volgere di pochi decenni): i droni armati, gli attacchi informatici e i sistemi d'arma autonomi.

2. I droni armati

Dato il loro impiego come strumento di attuazione dei programmi di uccisioni mirate (cd. *Targeted killings*), l'uso dei droni armati può considerarsi soggetto al regime generale che disciplina queste ultime nel diritto internazionale.[2] Tale regime consta di due sotto-regimi: uno applicabile nell'ambito dei conflitti armati (*conduct of hostilities*

[1] Cristopher GREENWOOD, *The Law of Weaponry at the Start of the New Millennium*, in M. SCHMITT e L.C. GREEN, L.C. (a cura di), *The Law of Armed Conflict: Into the Next Millenium*, Naval War College, Rhode Island 1998, pp. 221-222.

[2] Sul quale, v. in generale Nils MELZER, *Targeted Killing in International Law*, Oxford University Press, New York 2008.

paradigm), ed uno all'infuori di questi (*law enforcement paradigm*). Nel primo caso, le uccisioni mirate sono da ritenersi lecite a condizione che siano rispettati i principi di distinzione, proporzionalità e precauzione previsti dal diritto internazionale umanitario;[3] nel secondo, esse sono considerate come operazioni di polizia, con la conseguenza che saranno in linea di principio incompatibili con le norme internazionali che tutelano il diritto umano alla vita, salvo che non costituiscano l'unica misura praticabile per proteggere la vita e l'incolumità dell'agente e/o quella altrui da una minaccia illecita.[4]

La chiarezza del quadro normativo appena descritto appare gravemente offuscata nella prassi degli Stati che realizzano uccisioni mirate mediante droni, *in primis* gli Stati Uniti. Questi ultimi, difatti, tendono a qualificare – in modo del tutto improprio – la lotta globale al terrorismo come "conflitto armato", finendo così con l'applicare alle uccisioni mirate dei (sospetti) terroristi il regime meno restrittivo previsto dal diritto internazionale umanitario.[5] Peraltro, nella prassi più recente, l'uso dei droni armati è sempre più di frequente diretto contro presunti militanti, le cui generalità sono ignote, identificati ed attaccati sulla sola base di modelli comportamentali che ne suggerirebbero il coinvolgimento in attività di tipo terroristico (cd. *Signature strikes*). Sennonché, com'è stato accuratamente dimostrato, molti di questi criteri sono del tutto incompatibili, non solo con le (rigide) norme internazionali che proteggono il diritto alla vita, ma anche con i più permissivi principi del diritto internazionale umanitario (si pensi, su tutti, al criterio secondo cui sarebbero da considerarsi terroristi, e dunque obbiettivi legittimi, tutti gli uomini in età militare che si trovino in aree dove stanno operando, o hanno recentemente operato, gruppi terroristici).[6]

Queste preoccupanti tendenze rischiano di produrre interpretazioni distorte di un regime giuridico che, se correttamente inteso, offrirebbe una disciplina più che adeguata all'uso letale dei droni armati. Sotto questo profilo, appare particolarmente significativo che le obiezioni sollevate a livello internazionale contro l'uso dei droni nel quadro dei programmi di uccisioni mirate assumono per lo più la forma di una riaf-

---

[3] *Ibid.*, pp. 241-419.

[4] In questo senso, v. ad esempio il Principio 9 dei *Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*, adottati nell'ambito dell'ottavo congresso delle Nazioni Unite sulla prevenzione del crimine ed il trattamento dei trasgressori, tenutosi all'Avana (Cuba), dal 27 agosto al 7 settembre 1990.

[5] Anthony CULLEN, *The characterization of remote warfare under international humanitarian law*, in J.D. OHLIN (a cura di), *Research Handbook on Remote Warfare*, Edward Elgar Press, Cheltenham/Northampton 2017, pp. 117-120.

[6] Kevin J. HELLER, *'One Hell of a Killing Machine': Signature Strikes and International Law*, in "Journal of International Criminal Justice", n. 11, v. 1, anno 2013, p. 97.

fermazione dell'obbligo di rispettare i principi vigenti, piuttosto che della necessità di adottare nuove norme.[7]

3. Gli attacchi informatici

E' stato osservato che, sebbene la guerra cibernetica costituisse uno sviluppo "imprevisto (ed imprevedibile)" al momento della redazione delle Convenzioni di Ginevra e dei relativi Protocolli addizionali, tale circostanza non sarebbe di per sé idonea ad impedire l'applicazione dei principi in essi codificati anche agli attacchi informatici.[8] Tale approccio è ben esemplificato dal Manuale di Tallinn sul diritto internazionale applicabile alle operazioni informatiche, elaborato sotto gli auspici del Centro di eccellenza per la Cyber difesa della NATO.[9] Le sue "regole" (nella seconda edizione, ben 154) si sforzano di adattare l'intero *corpus* del diritto internazionale classico al dominio cibernetico mediante una serie di aggiustamenti di natura non sostanziale. Segnatamente, il Manuale sembra minimizzare alcune caratteristiche uniche di questa tipologia di conflitti, ed in particolare la "virtualità" dello spazio cibernetico, facendo leva sulle "territorialità" delle infrastrutture informatiche (v., in particolare, le Regole sulla sovranità: 1-5), e circoscrivendo la nozione di "attacco informatico" alle operazioni cibernetiche con potenziali effetti distruttivi nel mondo "fisico" (cioè "lesioni o morte alle persone o danni o distruzione di oggetti", v. la Regola 92 e il relativo commento). Secondo alcuni, incluso il Comitato internazionale per la croce rossa, tale definizione sarebbe troppo limitata, essendo essa inidonea a proteggere la popolazione civile da operazioni informatiche ostili risultanti *solo* nella cancellazione o alterazione di dati.[10] Inoltre, occorre tener presente che la perdita o la corruzione dei dati è un evento non meno "fisico" di altri, anche se i suoi effetti sono limitati a sistemi di computer e reti informatiche.

Un approccio più innovativo è stato recentemente proposto dal Presidente e *Chief Legal Officer* della Microsoft, Bradford Smith, il quale ha esortato gli Stati a negoziare

---

[7] V., tra gli altri, Risoluzione del Parlamento europeo del 27 febbraio 2014 sull'utilizzo di droni armati (2014/2567(RSP)); Cristof HEYNS, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, 1° aprile 2014, UN Doc. A/HRC/26/36, parr. 139-140; UN Human Rights Council, *Ensuring use of remotely piloted aircraft or armed drones in counterterrorism and military operations in accordance with international law, including international human rights and humanitarian law*, 15 aprile 2014, UN Doc. A/HRC/RES/25/22; Risoluzione dell'Assemblea Parlamentare del Consiglio d'Europa del 23 aprile 2015, *Drones and targeted killings: the need to uphold human rights and international law*, Resolution 2051 (2015)).

[8] Gary D. SOLIS, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge University Press, New York 2016, p. 702.

[9] Michael N. SCHMITT (a cura di), *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations*, Cambridge University Press, New York 2017.

[10] COMITATO INTERNAZIONALE PER LA CROCE ROSSA, *International humanitarian law and the challenges of contemporary armed conflicts. Report 32IC/15/11 for the 32nd International Conference of the Red Cross and the Red Crescent, Geneva, Switzerland, 8–10 December 2015*, Ginevra, 2015, p. 43.

una sorta di Convenzione di Ginevra "digitale" avente il duplice scopo di offrire una protezione specifica alle aziende informatiche e di assegnare ad esse il compito di assistere la popolazione civile contro gli attacchi informatici perpetrati dagli Stati.[11] La proposta di Smith prevede altresì l'istituzione di un'organizzazione internazionale, liberamente ispirata all'Agenzia internazionale per l'energia atomica, che affiancherebbe a tecnici di nomina governativa esperti provenienti dal settore privato, dal mondo accademico e dalla società civile, incaricata di esaminare i casi di attacchi informatici e rendere pubbliche le prove che ne dimostrano l'attribuibilità ad uno Stato.[12] Quest'ultimo aspetto tocca uno dei profili più problematici della disciplina internazionale dei ciberconflitti, vale a dire quello relativo all'attribuzione degli attacchi informatici. La possibilità tecnica di lanciare un'operazione cibernetica ostile assumendo fittiziamente l'identità di un altro Stato o di un'organizzazione internazionale (cd. *spoofing*) pone in effetti problemi probatori cui le norme classiche in materia di responsabilità internazionale non sono in grado di dare risposta. Per questo motivo, la circostanza che, sul punto, il Manuale di Tallinn si limiti a riproporre i tradizionali criteri di attribuzione (Regole 15-18) appare una soluzione che, sebbene formalmente corretta, si rivela ampiamente inadeguata a colmare una lacuna che rischia di minare alla base la possibilità stessa di reagire ad atti internazionalmente illeciti consistenti in operazioni informatiche.

Di fronte a queste sfide, è senz'altro deplorevole constatare lo scarso dinamismo e la sostanziale assenza di propositività delle iniziative intergovernative su questo tema. Facciamo in riferimento, in particolare, alla circostanza che i lavori del Gruppo di esperti governativi delle Nazioni Unite sugli sviluppi nel campo dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale versino in una situazione di stallo, non essendo stato possibile trovare un accordo su un punto apparentemente pacifico, vale a dire l'applicabilità alle operazioni cibernetiche ostili delle norme internazionali sull'uso della forza (divieto dell'uso della forza, diritto alla legittima difesa, diritto internazionale umanitario). Ad avviso di alcuni Stati, infatti, ciò avrebbe comportato il rischio di una destabilizzante "militarizzazione" del ciberspazio.[13]

4. I sistemi d'arma autonomi

A partire dal 2017, un altro Gruppo di esperti governativi ha avviato i propri lavori, si spera con maggior profitto. Dopo un ciclo triennale di incontri informali (2014-2016), gli Stati Parte della Convenzione sulle armi convenzionali hanno deciso di istituire un Gruppo di esperti governativi con il compito di esplorare possibili solu-

---

[11] Bradford SMITH, *The need for a Digital Geneva Convention. Keynote Address at the RSA Conference 2017*, 14 febbraio 2017.

[12] *Ibid*.

[13] Arun M. SUKUMAR, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, in "Lawfare", 4 luglio 2017.

zioni normative ai problemi posti dai sistemi d'arma autonomi. Secondo la definizione offerta dal Comitato internazionale per la croce rossa (ed intorno alla quale si sta formando un crescente consenso), i sistemi d'arma autonomi sono quelli "in grado di selezionare ed attaccare gli obbiettivi in modo indipendente, vale a dire con autonomia nelle funzioni critiche della acquisizione, tracciamento, selezione ed ingaggio degli obbiettivi".[14] E' bene evidenziare come, nella misura in cui il tratto saliente di questa innovazione tecnologica risiede nella tecnica di identificazione degli obbiettivi e non nell'arma in sé,[15] l'autonomia è una proprietà che può essere in principio implementata in qualsiasi tipologia di arma, inclusi i droni e le armi informatiche.

Il dibattito pubblico sulle implicazioni etico-giuridiche poste dai sistemi d'arma autonomi è stato promosso dalla Campagna "Stop Killer Robots", lanciata nel 2013 da una coalizione internazionale di ONG con l'obiettivo primario di vietare le armi robotiche letali.[16] Nello stesso anno, il Relatore speciale delle Nazioni Unite sulle esecuzioni extragiudiziali, sommarie o arbitrarie, Christof Heyns, ha pubblicato un rapporto sui sistemi d'arma autonomi che ha fortemente influenzato la successiva discussione sul tema, sia in sede accademica che diplomatica, in ragione della chiara identificazione dei principali problemi in gioco,[17] ovvero: *i)* le norme di diritto internazionale che disciplinano la selezione e l'ingaggio degli obbiettivi (il cd. *targeting*), ed in particolare i principi di distinzione e proporzionalità, implicherebbero capacità che sono proprie dell'essere umano e non sono replicabili da una macchina, vale a dire la capacità di acquisire consapevolezza situazionale e quella di formulare giudizi qualitativi (paragrafi 63-74); *ii)* attraverso la rimozione degli operatori umani dal processo decisionale, l'autonomia nei sistemi d'arma renderebbe più complessa—quando non impossibile—l'imputazione della responsabilità giuridica in caso di eventi dannosi (paragrafi 75-81); *iii)* l'impiego di sistemi d'arma autonomi letali costituirebbe un oltraggio alla dignità umana, la quale impone che l'assunzione di decisioni di vita o di morte non possa essere delegata a decisori non-umani (paragrafi 89-97); iv) l'autonomia nei sistemi d'arma potrebbe essere fonte di instabilità a livello internazionale, in quanto azzererebbe il "costo" politico solitamente connesso all'inizio di una campagna militare (i.e. il rischio di perdite tra le proprie forze) (paragrafi 57-62).

---

[14] COMITATO INTERNAZIONALE PER LA CROCE ROSSA, *Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Expert meeting, Geneva, Switzerland, 26-28 March 2014*, Ginevra, 2014, p. 5. Per una disamina delle varie proposte di definizione dei sistemi d'arma autonomi v. Daniele AMOROSO, Frank SAUER, Noel SHARKEY, Lucy SUCHMAN e Guglielmo TAMBURRINI, *Autonomy in Weapon Systems. The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy*, Grossbeeren, Berlino 2018, pp. 19-22.

[15] Kjølv EGELAND, *Lethal Autonomous Weapon Systems under International Humanitarian Law*, in "Nordic Journal of International Law", n. 85, v. 2, anno 2016, p. 97.

[16] *Urgent Action Needed to Ban Fully Autonomous Weapons. Non-governmental organizations convene to launch Campaign to Stop Killer Robots*, 30 maggio 2013.

[17] Cristof HEYNS, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, 9 aprile 2013, UN Doc. A/HRC/23/47.

La discussione tra gli Stati parte della Convenzione sulle armi convenzionali è stata caratterizzata dal contrasto tra coloro che ritengono il quadro giuridico vigente idoneo a risolvere i problemi testé menzionati e coloro che invece sollecitano l'adozione di nuove norme, vuoi nella forma di un regime *ad hoc*, vuoi come divieto assoluto sullo sviluppo, la produzione e l'utilizzo delle armi autonome. Nel corso degli anni, tuttavia, un certo consenso si è condensato intorno all'idea secondo cui tutte le armi (inclusi i sistemi d'arma autonomi) dovrebbero essere soggette ad un "controllo umano significativo" (CUS).[18] A ben vedere, la nozione di CUS può coprire il divario tra le varie posizioni espresse sinora in seno al Gruppo di esperti governativi. Si tratta di un principio desumibile dal quadro giuridico esistente, ma che necessita al tempo stesso di nuove norme che ne specifichino il contenuto e lo rendano operativo. Inoltre, un protocollo alla Convenzione sulle armi convenzionali che imponesse il requisito del CUS potrebbe essere considerato, al contempo, come una forma di regolamentazione ed un divieto all'implementazione della (piena) autonomia sulle funzioni critiche dei sistemi d'arma.[19] Per questo motivo, la nozione di CUS—e più in generale quella di "controllo umano"—è generalmente vista come idonea a consentire la prosecuzione dei negoziati e l'adozione di uno strumento (auspicabilmente vincolante) nel quadro della Convenzione.[20]

Ma cos'è che rende il controllo umano sui sistemi di armi veramente "significativo"? Indubbiamente, questo punto cruciale rimane ancora largamente irrisolto. La nostra ipotesi di ricerca—che cercheremo di meglio articolare in futuri scritti—è che questo problema non si presta ad un'unica soluzione, valida per tutti i sistemi d'arma e per tutti gli scenari, essendo piuttosto necessario un approccio differenziato, ancorché fondato su principi etici e giuridici comuni.[21] I principi su cui dovrebbe basarsi la nozione di CUS sono già stati menzionati sopra: il controllo umano sui sistemi d'arma dovrebbe garantire il rispetto delle norme internazionali in tema di *targeting*; dovrebbe evitare vuoti di responsabilità in caso di eventi dannosi; non dovrebbe consentire ad una macchina di operare scelte morali riguardanti la vita, l'integrità fisica e i beni delle persone coinvolte in un conflitto armato (o in altro contesto in cui l'arma può essere impiegata); non dovrebbe rappresentare una minaccia per la pace e la sicurezza internazionale.

---

[18] V., da ultimo, Risoluzione del Parlamento europeo del 12 settembre 2018 sui sistemi d'arma autonomi (2018/2752(RSP)), in particolare parr. 2-4.

[19] Nehal BHUTA, Susanne BECK e Robin GEISS, *Present Futures: Concluding Reflections and Open Questions on Autonomous Weapons Systems*, in N. BHUTA et al (a cura di), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Cambridge 2016, p. 381.

[20] UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR), *The Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control might move the discussion forward,* 2014.

[21] Per una prima esposizione, v. Daniele AMOROSO e Guglielmo TAMBURRINI, *The Ethical and Legal Case Against Autonomy in Weapons Systems*, in "Global Jurist", n. 17, v. 3, anno 2017, DOI: https://doi.org/10.1515/gj-2017-0012, pp. 13-14.

L'applicazione di questi principi in situazioni concrete dovrebbe essere, a nostro avviso, facilitata attraverso la formulazione di un adeguato insieme di regole che colleghino i primi alle seconde. Queste "regole-ponte" dovranno avere una classica struttura binaria, costituita da *fattispecie* e *statuizione* (se A, allora B). Segnatamente, la "fattispecie" sarà integrata dalla combinazione di una serie di fattori, vale a dire gli obbiettivi operativi assegnati all'arma (offensivi/difensivi), la cornice geografica e temporale nella quale essa è chiamata a funzionare senza controllo umano, le caratteristiche dello scenario operativo (e.g. presenza/assenza di civili), la tipologia di obbiettivi da ingaggiare (persone, oggetti "abitati", oggetti "disabitati"). Per ciascuna combinazione di questi fattori, andrà individuata una "statuizione" consistente nel livello di controllo umano normativamente richiesto come "significativo". A questo proposito, si potrebbe pensare—ma la proposta andrà meglio sviluppata—a quattro livelli di interazione tra operatore ed arma (attivazione, supervisione e veto, approvazione del singolo attacco proposto dalla macchina, scelta deliberata dell'essere umano) i quali, alla luce dei principi sopra richiamati, saranno considerati di volta in volta sufficienti a garantire un controllo umano significativo sull'arma nelle diverse fattispecie considerate, nonché ad assicurare un nesso tra azione umana ed evento dannoso idoneo ad incardinare un rapporto di responsabilità. In questo modo, l'eventuale autonomia "residua" dei sistemi d'arma sarebbe eticamente e giuridicamente accettabile in quanto "depurata" degli aspetti problematici derivanti dall'esecuzione incontrollata delle funzioni critiche della selezione e dell'ingaggio degli obbiettivi.

I 10 *Possible Guiding Principles* adottati dal Gruppo di esperti governativi all'esito del suo ultimo incontro (27-31 agosto 2018) sembrano andare timidamente in questa direzione.[22] Di particolare interesse per la nostra discussione appaiono, in particolare, il Principio 2, in cui si ribadisce la necessità di assicurare la "responsabilità umana" per le decisioni riguardanti l'impiego dei sistemi d'arma ed il Principio 3, il quale specifica che la garanzia di una responsabilità siffatta passa per il mantenimento di "una catena responsabile di comando e controllo." Come chiunque può vedere, tuttavia, si tratta di indicazioni molto vaghe, la cui idoneità a gettare le basi per una regolamentazione efficace dipende in ultima analisi dall'adozione di "regole-ponte" più dettagliate del tipo sopra descritto.

6. Conclusioni

L'analisi che precede conferma solo in parte le previsioni formulate da Greenwood sul finire dello scorso millennio. Il fedele rispetto della *lex lata* costituisce senz'altro un valido punto di partenza per affrontare le implicazioni etico-giuridiche delle nuove tecnologie in campo militare. Questo è certamente il caso, come abbiamo avuto modo di vedere, dell'uso letale dei droni armati. A volte, tuttavia, il diritto vigente può rivelarsi insufficiente ad offrire risposte adeguate a problemi che non sono riducibili all'interno dell'armamentario normativo tradizionale: si pensi, in proposito, alla que-

[22] *Report of the 2018 Group of Governmental Experts on Lethal Autonomous Weapons Systems*, 31 agosto 2018, UN Doc. CCW/GGE.2/2018/3, Parte IV.A.

stione dell'attribuzione degli attacchi informatici o alla necessità di definire in dettaglio il requisito del controllo umano significativo. Elaborare soluzioni creative e appropriate a questi problemi, senza disperdere il patrimonio giuridico del passato, è forse una delle sfide più importanti per la comunità internazionale contemporanea.

Nota Bibliografica

Daniele AMOROSO e Guglielmo TAMBURRINI, *The Ethical and Legal Case Against Autonomy in Weapons Systems*, in "Global Jurist", n. 17, v. 3, anno 2017, DOI: https://doi.org/10.1515/gj-2017-0012.

Daniele AMOROSO, Frank SAUER, Noel SHARKEY, Lucy SUCHMAN e Guglielmo TAMBURRINI, *Autonomy in Weapon Systems. The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy*, Grossbeeren, Berlino 2018.

Basic Principles on the Use of Force and Firearms by Law Enforcement Officials Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August to 7 September 1990, Cuba 1990, https://www.ohchr.org/en/professionalinterest/pages/useofforceandfirearms.aspx.

Nehal BHUTA, Susanne BECK e Robin GEISS, *Present Futures: Concluding Reflections and Open Questions on Autonomous Weapons Systems*, in N. BHUTA et al (a cura di), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Cambridge 2016, pp. 347-382.

COMITATO INTERNAZIONALE PER LA CROCE ROSSA, *Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Expert meeting, Geneva, Switzerland, 26-28 March 2014*, Ginevra 2014, https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014.

COMITATO INTERNAZIONALE PER LA CROCE ROSSA, *International humanitarian law and the challenges of contemporary armed conflicts. Report 32IC/15/11 for the 32nd International Conference of the Red Cross and the Red Crescent, Geneva, Switzerland, 8–10 December 2015*, Ginevra 2015, http://rcrcconference.org/wp-content/uploads/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf.

Anthony CULLEN, *The characterization of remote warfare under international humanitarian law*, in J.D. OHLIN (a cura di), *Research Handbook on Remote Warfare*, Edward Elgar Press, Cheltenham/Northampton 2017, pp. 110-132.

Kjølv EGELAND, *Lethal Autonomous Weapon Systems under International Humanitarian Law*, in "Nordic Journal of International Law", n. 85, v. 2, anno 2016, pp. 89-118.

Cristopher GREENWOOD, *The Law of Weaponry at the Start of the New Millennium*, in M. SCHMITT e L.C. GREEN, L.C. (a cura di), *The Law of Armed Conflict: Into the Next Millenium*, Naval War College, Rhode Island 1998, pp. 185-231.

Cristof HEYNS, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, 9 aprile 2013, UN Doc. A/HRC/23/47. https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf.

Cristof HEYNS, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, 1° aprile 2014, UN Doc. A/HRC/26/36. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/128/20/PDF/G1412820.pdf?OpenElement.

Kevin J. HELLER, *'One Hell of a Killing Machine': Signature Strikes and International Law*, in "Journal of International Criminal Justice", n. 11, v. 1, anno 2013, pp. 89-119.

Nils MELZER, *Targeted Killing in International Law*, Oxford University Press, New York 2008.

Report of the 2018 Group of Governmental Experts on Lethal Autonomous Weapons Systems, 31 agosto 2018, UN Doc. CCW/GGE.2/2018/3. https://www.unog.ch/80256EDD006B8954/(httpAssets)/20092911F6495FA7C125830E003F9A5B/$file/2018_GGE+LAWS_Final+Report.pdf.

Risoluzione del Parlamento europeo del 27 febbraio 2014 sull'utilizzo di droni armati (2014/2567(RSP)). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P7-RC-2014-0201+0+DOC+XML+V0//EN.

Risoluzione del Parlamento europeo del 12 settembre 2018 sui sistemi d'arma autonomi (2018/2752(RSP)). http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0360&language=EN.

Risoluzione dell'Assemblea Parlamentare del Consiglio d'Europa del 23 aprile 2015, *Drones and targeted killings: the need to uphold human rights and international law*, Resolution 2051 (2015)). http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21746.

Michael N. SCHMITT (a cura di), *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations*, Cambridge University Press, New York 2017.

Bradford SMITH, *The need for a Digital Geneva Convention. Keynote Address at the RSA Conference 2017*, 14 febbraio 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Gary D. SOLIS, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge University Press, New York 2016.

Arun M. SUKUMAR, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, in "Lawfare", 4 luglio 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

UN HUMAN RIGHTS COUNCIL, *Ensuring use of remotely piloted aircraft or armed drones in counterterrorism and military operations in accordance with international law, including international human rights and humanitarian law*, 15 aprile 2014, UN Doc. A/HRC/RES/25/22. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/25/L.32.

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR), *The Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control might move the discussion forward*, 2014. http://www.unidir.org/files/publications/pdfs/considering-how-meaningful-human-control-might-move-the-discussion-forward-en-615.pdf.

Urgent Action Needed to Ban Fully Autonomous Weapons. Non-governmental organizations convene to launch Campaign to Stop Killer Robots, 30 maggio 2013, http://stopkillerrobots.org/wp-content/uploads/2013/04/KRC_ LaunchStatement_23Apr2013.pdf.