Medicine, Conflict and Survival

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fmcs20

Information technology for peace and security: IT applications and infrastructures in conflict, crises, war and peace

edited by Christian Reuter, Heidelberg, Springer, 2019, 424 pp., £27.99 (paperback), ISBN 978-3-658-25651-7; £26.74 (ebook), ISBN 978-3-658-25652-4

Marion Birch

To cite this article: Marion Birch (2020) Information technology for peace and security: IT applications and infrastructures in conflict, crises, war and peace, Medicine, Conflict and Survival, 36:3, 272-274, DOI: 10.1080/13623699.2020.1742960

To link to this article: https://doi.org/10.1080/13623699.2020.1742960

Published online: 24 Mar 2020.

Submit your article to this journal

Article views: 30

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=fmcs20

Information technology for peace and security: IT applications and infrastructures in conflict, crises, war and peace, edited by Christian Reuter, Heidelberg, Springer, 2019, 424 pp., £27.99 (paperback), ISBN 978-3-658-25651-7; £26.74 (ebook), ISBN 978-3-658-25652-4

This is a textbook and so does not necessarily invite reading from beginning to end. But this is an area where knowledge, concepts and language are growing so fast that – at least for someone with a relatively limited knowledge of information technology (IT) – it was well worth doing. The authors clarify links between information technology and everyday situations in an engaging way and there is clear signposting and cross referencing to keep the reader on track and – in many places – concerned.

Information Technology for Peace and Security is written by 27 contributors from 12 universities and institutes; several authors are from the Technische Universität of Darmstadt where the Editor holds a Chair in Science and Technology for Peace and Security and a secondary post in history and social sciences. Sections cover Cyber Conflicts and War, Cyber Peace, Cyber Arms Control, Cyber Attribution and Infrastructures, and Culture and Interaction. Sub-sections are clearly described in the Introduction and Overview for readers who want to pursue a particular issue.

It is clear from the start that although this is a relatively new area it builds on previous work on conflict prevention and peace, with sections on Verification in Cyberspace and Arms Control and its Applicability to Cyberspace. The Introduction firmly links cyberspace to the history of natural science and technical peace research; it outlines both the challenges and opportunities for scientists concerned with peace to use the same IT knowledge that is changing the face of war to prevent it.

Part II covers cyber warfare, cyber espionage and defence, and darknets. The US military aspires to Information Dominance 'whether in peace, conflict or war' so by definition this stretches 'well into the civilian domain in peacetime' (66); that there have been mutual attempts to agree deterrence and stabilizing measures in this area since 2013 is only mildly reassuring. The discussion of cyber espionage concentrates on actors who have a mandate to conduct espionage on behalf of a nation state – and points out that nation states invest much more in this activity than 'ordinary' criminals. The chapter on Darknets as Tools for Cyber Warfare includes an illuminating section on how darknets can feed into the process of securitization and speed up the securitization and militarization of data networks.

Part III covers cyber peace and expands on the 14 demands of the cyber peace campaign of the Forum of Computer Scientists for Peace and Social Responsibility. These respond to challenges of dual-use and imprecise definitions (for example: when does malware qualify as a weapon?) as well as a general atmosphere of distrust in the sector. A voluntary commitment (the Civil Clause) and questionnaire developed by the Technische Universität of Darmstadt provides a practical example of how academics can be helped to decide if their research is truly as 'non-military' as it can be. Accepting that cyber arms control presents new and daunting challenges the importance of confidence and security building measures to reduce mistrust and threats is stressed.

Despite the challenges Section IV considers arms control in cyberspace, including unmanned systems and verification. A short history of arms control, particularly as it relates to nuclear weapons, emphasizes key issues and is the background to a description of multi-lateral and state level efforts to date to control a universally recognized threat to critical infrastructure. The chapter on autonomous weapons systems – a term for which there is as yet no agreed definition – concentrates on the legal, ethical, practical and psychological problems they present, and differentiates between those that are programmed to kill rather than those that might kill as part of collateral damage. How do you program international humanitarian law into their controlling software and deal with the problem of automation bias – the human tendency to agree with actions suggested by a computer? Arms control inevitably leads to a discussion of verification and the difficulties of adapting verification procedures used for other weapons to cyberspace. These include deciding whether potential activity will be aggressive or defensive – something that is particularly difficult given the dual-use nature of IT goods.

Cyber Attribution and Infrastructures is perhaps the hardest section to understand for readers with limited IT knowledge. There are some amusing similarities to more conventional intelligence work with the use of honeypot computers posing as average phones. It is reassuring that retaliation following attribution is often avoided to prevent escalation, particularly as the cyberwar concepts of both the US and China indicate that a conventional strike should be carried out shortly after a cyber attack if a military objective is to be successful. The political and legal dimensions of attribution are briefly discussed, and a very human challenge with some arguing that 'attribution is what a state makes of it' (299) i.e. that a political decision will have to be taken to decide what level of evidence is needed before a reaction can take place. Everyday networks that collect and disseminate massive amounts of data are discussed in the chapter on critical information infrastructures, including possible protection measures against a range of threats including those that could cause ripples and escalation.

Perhaps most relevant for readers of MCS are the chapters on safety and security, cultural violence and peace in social media, and social media and ICT usage in conflict areas. The areas of safety, security and politics increasingly overlap; individuals with the technological expertise that traditionally dealt with safety issues now need to also understand the cultural and political factors behind security considerations. The potential for cultural violence in social media is brought chillingly home when a leader of a far-right party says: 'If the message fits we actually don't care where it's coming from [. . ..] it's no big deal if it's fake.'(366). Several ways that fake news and content that is intentionally fabricated, manipulated or misinterpreted, including by social bots, can be detected and challenged are described – and in some tasks humans are still better than machines. Four conflict case studies concentrate on how social media and ICT has been used by activists and opposition groups, and on how governments can try to shut this down. The need for a critical perspective in the analysis of social media content, including from activists, is mentioned despite the power asymmetry they face in conflict situations.

In the final Outlook section the editor and nineteen of the other authors give their forecast for the next 5–15 years. Despite being cautious and explaining that they are sometimes expressing what they think should be done, rather than what may happen, this is concerning reading. Cyberspace is recognized as a military domain and a cyber arms race is already well under way with dedicated resources that far exceed those given to attempts to control it – such as the work described here. The particular characteristics of IT technology are challenging: difficulty in attribution, easy duplication, dual use and the close relationship between military and civilian technology. Autonomous weapons systems are a particular concern. Nevertheless the practical suggestions for what needs to be done are clearly laid out and recognize that anything technical will have to be underwritten by peaceful intentions and trust developed through agreed verification and information sharing.

Excellent as this book is the reader is left with the impression that those who understand what is at stake are running to keep up. NATO has already decided that attacks in cyberspace can invoke Article V of the NATO Charter, despite no clear agreement having been reached on what cyber activity – in terms of destructive potential and impact – would register as an attack. There are interesting attempts to relate aspects of cyber warfare to international humanitarian law (when would a hacker qualify as a combatant? what constitutes an armed attack?) and these could perhaps have been explored a little more as IHL is also grappling with issues of modern warfare.

Should you buy this book as a textbook – definitely. Should you buy it to read through or dip into if you are not learning about IT – definitely. This is a fast-developing area of knowledge with significant implications for peace and armed conflict – we can't all be experts, but we all need to understand as far as possible what needs to be done.

Marion Birch
Medact & Institute for Global Health, University College London
marion.birch2@btinternet.com

© 2020 Marion Birch
https://doi.org/10.1080/13623699.2020.1742960

Check for updates

The Oxford handbook of ethics of war, edited by Seth Lazar and Helen Frowe, Oxford, Oxford University Press, 2018, 592 pp., £97.00 (hardback), ISBN 9780199943418, also available at Oxford Handbooks Online (https://www.oxfordhandbooks.com)

This tome continues the Oxford Handbook series which aims to capture contemporary thinking on a particular subject. This one, on the ethics of war, certainly achieves this.