Currently the terms ‘hacktivism’, ‘digital activism’ and ‘cyber activism’ are frequently used by the various global media outlets, especially in connection with the social media-enabled protests taking place in the Middle East, Europe and elsewhere around the world. Understanding the nuances of these terms, their relationship to cyberconflict, and the difficulties for governments and the international community in responding to any type of cyberconflict incident are well worth exploring at this point in time.

Hacktivism is a term that combines the words hacker and activism. It refers to the art of manipulating code and using computers for political purposes. These include mobilizing supporters, creating software that helps bypass censorship or bridge digital inequality, and supporting specific campaigns, organizations, and protests around the world using electronic disobedience or social mobilization. Hacktivism in its purest form is an information-age ideology which, depending on the political spectrum, can support: peer production as an alternative mode to capitalism, copyleft or open source software, direct or participatory democracy, and transparent government. Nevertheless, despite their general similarities, online activist groups adhere to various ideological lines that can range towards libertarianism, anarchist principles, and left wing politics, or may support more conservative causes by advocating right-wing individualist free markets, or even promote ultra-right wing causes. This is why these phenomena are identified under the general idea of cyberconflict. In cyberconflict individuals and groups engage in computer-mediated conflicts that span ethno-religious, cultural and sociopolitical conflicts and causes.

Historically, we are witnessing a transfer of conflicts around the world through cyberspace during cyberconflict incidents. Examples include the Israeli-Palestinian conflict, the Iraq War, Al-Qaeda and many more. These can also be sociopolitical and economic conflicts, such as the anti-globalization movement, the anti-war movement, or social protests that use social media with the intent of promoting change. The relevance of the use of technological innovation is beyond critical at the moment. Social media networking is being used to accelerate regime changes in the Middle East and elsewhere. The undeniable public nature of the plight of citizens in these states communicated through the virtual public sphere has forced the international community to respond with military interventions to protect them. This response is a prelude of things to come.

Individuals and groups that engage in cyberconflict are informed by different ideologies. Hacktivism is one such phenomenon. Normally hacktivists tend to be influenced by traditional ideologies as we know them. Still hacktivism in its ethical form does not support the destruction of online spaces or condone online intrusions unless digital spaces are used for forms of electronic disobedience as social protest. To clarify: the use of cyber attacks is a topic of debate among hacktivist groups as to
whether it is ethical to disrupt someone else’s freedom of expression for instance. I would say that politically informed hacktivism promotes causes that adhere to freedom of information, the promotion of copyright-free products and the use of technology to change the global system for the better by introducing tools, spaces and forums, to name a few forms, that enable transparent government, peer production as an alternative to capitalism, and promote global digital rights, especially against state censorship. Digital activism or cyber-activism that adheres to fixed notions of state, religion, homeland, nationalism, racism and so on, tends, in my view, to use new media for the more traditional purposes of propaganda and hatred, and often supports fascist notions of politics and existence in general. I would suggest ending the use of the term hacktivism for these types of individuals and movements in favour of terms such as online hatred, cybernationalism, online propaganda and others that accentuate this difference. As a network structure, the internet is compatible with network structures of organization and mobilization. This is why hacktivism in its purest form stems from information-age ideologies that enable future horizontal and networked forms of governance and alternative modes of production. This type of hacktivism is forward-looking, and not disruptive purely for the sake of it, nor does it support hatred, racism or discrimination.

The term ‘hacker’ was coined in the US in the 1960s to refer to a virtuoso of technology who programs enthusiastically and stretches technology. Since then it has seen many uses. In most mainstream media and the common parlance, all computer-system intruders are referred to as hackers. Hacker communities, however, have agreed on clear distinctions and those engaged in cybercrime are crackers, phrackers, cybercriminals, or black hat hackers. Some hackers are politically active, others are not. A hacker’s status as hacktivist depends on the extent of that individual’s political engagement and competence. To me political maturity and positive engagement makes for a hacktivist worth their code and our time.

In recent riots in the United Kingdom, where I am based, teenagers were prosecuted disproportionately often for ‘inciting violence through social networking sites’. Teenagers are immersed in cyberspace in the advanced knowledge economies at the core of the global village, an experience slowly spreading across the globe despite the economic inequalities perpetuated by the current system. It is obvious that this results in cyberspace playing a critical role in the everyday activities of young people. The need to be respected, to be acknowledged and participate in the world around us can often be pressing at that age, but this is generally all that is really going on for teenage hackers. I also don’t think their cyber behaviour stems from boredom or lack of a personal or social life. I think cyberspace is a natural affective extension for many young people and some find it powerful, challenging and socially rewarding to stretch a technology that their parents are not always comfortable with. Teenage hackers in particular express online what they cannot express offline. Because we live in a banal and consumerist world, they have the power to exert influence even in disruptive and script-kiddie ways, to prove they are also worthy of being included in the microphysics of power in everyday life. In a system in global crisis, it is unsurprising the many talented individuals are frustrated and rightly so. The more politically informed teenage hackers eventually find their way into progressive teams working in support of alternative forms of government and social movement organizations.
The ones who never leave puberty continue to vandalize cyberspace aimlessly or eventually enter cybercrime gangs for profit if there are no other alternatives.

In addition to this commentary on contemporary issues involved with online conflicts, there has been a pre-occupation over the last decade with cyberconflict in general and that tied to the revolution taking place in military affairs in particular. This in turn has highlighted the effects of information and communications technologies (ICTs) on global security beyond the more netwar, societal type of ethno/religious/cultural and socio/politico/economic uses of digital technologies in organizing, mobilizing, recruiting, and funding social movements, dissident groups and civil society actors. Historical incidents of cyberconflict by the ad hoc mobilization of non-state actors that accompany actual warfare, such as the one witnessed in Georgia during the conflict with Russia over South Ossetia, raise questions of cybersecurity as an element of global security. Unless the precise stage at which a cyber attack becomes part of an armed conflict is eventually defined by international law, any cyber attack could be classified a cybercrime and prosecuted as such. This is turn would mean that any political hacking even for protest purposes could be prosecuted as cybercrime, as indeed it has been by various governments against their own citizens. This could potentially mean that electronic disobedience or hacktivism as we have known it, despite having mostly symbolic effects, could also be prosecuted under this logic. Another problem for global politics is the difficulty in understanding where attacks originate from and whether they come from are state-sponsored or ad hoc assemblages. Not having defined the level where a cyber attack becomes the equivalent of an armed attack, there is no way currently to plan a reaction on an international level. Furthermore, its is not clear whether cyber attacks and cyber espionage will eventually be considered a form of war since information warfare and espionage historically have not been recognized as war or grounds for war.

Although it is impossible to predict the future of warfare, cyberconflict, the role of networks, and communication technology infrastructures will be of paramount importance, not only in the way wars are fought, but also in the way wars are communicated and justified in global public sphere. Digitally virtually enabling people to grasp political opportunity when ad hoc assemblages, protest networks and other resistance movements create cracks in the global political structure, such as the WikiLeaks situation and its effect on diplomacy and the spill-over effects in the Middle East right now, accelerates protests and points to the critical importance of political communication for the global transformations currently taking place. The move to overthrow repression, violence and fear through peaceful means and virtual protest and its real-life materialisation as revolution seems to be turning war into an extraordinary response to be used only to protect and not harm life. The politics of justifying war beyond the protection of life will likely be debated for a long time to come, but the importance of ICTs as a factor in the political communication of future wars, protests and resistance movements is unquestionable.

DDD #05 securing peace
For more see:

Books:

