RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS WORKING PAPER

**NO. 315**

# IS USE OF CYBER-BASED TECHNOLOGY IN HUMANITARIAN OPERATIONS LEADING TO THE REDUCTION OF HUMANITARIAN INDEPENDENCE?

**MARTIN STANLEY SEARLE**

**S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES**
**SINGAPORE**

**11 JUNE 2018**

# Abstract

Technologies of the Fourth Industrial Revolution (4IR) are being tested and adopted at a significant rate in humanitarian emergency response. However, the crossing of physical, biological, and cyber domains that characterises these technologies threatens the independence of humanitarian organisations. This is occurring in an environment in which the value and purpose of independence is already seriously questioned, both in practice, and in principle. This paper argues that the loss of independence stems from two related trends. First, several 4IR technologies are improving the capacity of humanitarian organisations to gather, synthesise, and analyse data, resulting in the production of information of increasingly strategic, political or military value. Second, the cyber component of these technologies simultaneously renders that information more vulnerable to unauthorised access by third parties with relevant political, military or economic agendas. This parallels the "capability/ vulnerability paradox" identified in literature discussing cybersecurity in relation to the military or so-called "smart cities". In conflict and disaster settings, this paradox increases the likelihood of humanitarian actors functioning as appendages of other organisations. This loss of independence potentially has operational implications relating to access, and material impact on the ongoing debate around the importance of independence in humanitarian work.

# Introduction

The Fourth Industrial Revolution (4IR) undergirds an "innovation turn" in the humanitarian sector. With increasing frequency, unmanned aerial vehicles are beaming data directly to software programmes, producing real-time maps of disaster affected areas and populations *in extremis*; and artificial intelligence is combing social media posts stemming from conflict and disaster zones to aid responders in their decision-making, as well as analysing mobile phone usage data to predict key demographic variables related to vulnerability. Elsewhere, bodies are being digitised in the name of effectiveness and accountability of aid distributions, and refugee governance. The Internet of Things (IoT) is improving the transportation of temperature sensitive vaccines, the treatment of patients with highly infectious diseases, and emergency supply chain management, while additive manufacturing is reducing the need to transport items over long distances, and, with computer-aided design, increasing the adaptability of operational logistics to specific contexts.

These innovations have prompted excitement among practitioners and policymakers alike, and a growing critical literature on risks to vulnerable populations,[1] [2] [3] [4] [5] [6] [7] and to the neutrality of humanitarian organisations.[8] [9] [10] [11] [12] Less attention has been paid to the related humanitarian principle of independence beyond references in the International Committee of the Red Cross' *Handbook on Data Protection in Humanitarian Action*.[13] The advent of 4IR technologies in humanitarian settings arguably creates important structural challenges to independence that require further exploration given the role of that principle in the negotiation of access to humanitarian aid.

[1] Hosein, Gus, and Carly Nyst. "Aiding surveillance: an exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries." (2013).

[2] Duffield, Mark. "The resilience of the ruins: towards a critique of digital humanitarianism." *Resilience* 4, no. 3 (2016): 147-165.

[3] Scott-Smith, Tom. "Humanitarian neophilia: the 'innovation turn'and its implications." *Third World Quarterly* 37, no. 12 (2016): 2229-2251.

[4] Jacobsen, Katja Lindskov. "Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees." *Security Dialogue* 46, no. 2 (2015): 144-164.

[5] Sandvik, Kristin, and Nathaniel A. Raymond. "Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response." (2017).

[6] Greenwood, Faine, Howarth, Caitlin, Poole, Danielle Escudero, Raymond, Nathaniel A., and Daniel P. Scarnecchia. "The Signal Code: A Human Rights Approach to Information During Crisis." *Harvard Humanitarian Initiative* (2017): www.hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis

[7] Mcdonald, S. M. "Ebola: a big data disaster." *Privacy, property, and the law of disaster experimentation. CIS Papers* (2016).

[8] Burns, Ryan. "Moments of closure in the knowledge politics of digital humanitarianism." *Geoforum* 53 (2014): 51-62.

[9] Jacobsen, Katja Lindskov. *The politics of humanitarian technology: good intentions, unintended consequences and insecurity*. Routledge, 2015.

[10] Byrne, Rory. "Trends in intelligence gathering by governments." In *Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF) Google Scholar*. 2016.

[11] Gilman, Daniel. "Cyber-Warfare and Humanitarian Space." In *Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF)*. 2014.

[12] Sandvik, Kristin Bergtora. "The humanitarian cyberspace: shrinking space or an expanding frontier?" *Third World Quarterly* 37, no. 1 (2016): 17-32.

[13] Kuner, Christopher Barth, and Massimo Marelli. "Handbook on data protection in humanitarian action." (2017).

The paper begins by drawing out the critical dividing lines in the discourse on humanitarian independence, highlighting that while it is conventionally considered one of the four core humanitarian principles, its value and application is highly contested. Against this backdrop, the paper argues that 4IR technology is challenging the feasibility of independence by highlighting two trends. First, several of these technologies are improving the capacity of humanitarian organisations to gather, synthesise, and analyse data, resulting in the production of information of increasingly strategic political, economic or military value. Second, the nature of 4IR technologies simultaneously makes that information more accessible to others with agendas other than humanitarian ones. The paper concludes by considering implications of this within the broader discussion around independence in humanitarianism.

## Independence and its Contestation

Independence is one of the four principles constituting specifically humanitarian action in the classic sense embodied by the International Committee of the Red Cross (ICRC), and labelled “Dunantist” after Jean Henri Dunant, the founder of the organisation. The remaining three are humanity, impartiality, and neutrality. These principles are not simply abstract values; they provide the language for aid workers to explain what they are doing and justify why they are doing it. This is routinely employed in negotiations with various stakeholders who can block a humanitarian organisation from providing aid to convince them to allow assistance to be delivered. As such, perhaps more than any other field, the principles underlying humanitarianism have immediate practical application.

Academic discourse on these principles tends to categorise independence, together with neutrality, as qualitatively distinct from humanity and impartiality, placing the latter two hierarchically above the former. For Jean Pictet, credited with developing much of the theory grounding the humanitarian principles, impartiality and humanity are the substantive principles defining what humanitarian action specifically is.[14] Following the European Commission’s Humanitarian Aid Office (ECHO), this means addressing human suffering wherever it is found, and doing so on the basis of the severity of need alone.[15] Neutrality and independence then serve as instruments to achieve the two substantive principles in the sorts of contested and chaotic contexts in which humanitarian need typically arises. Similarly, for Hugo Slim, head of policy at the ICRC and another long-time commentator on humanitarian principles, the first two principles concern what is a good action, while the second two concern how that good action is achieved.[16] This underscores the absoluteness of the first two principles, leaving little room for compromise, in contrast to the instrumentality of the second two, which allows for more flexibility that may be required in pursuit of the substantive principles. This relative flexibility is crucial to underscore; while Slim notes that independence and neutrality often do

[14] Pictet, Jean. "The fundamental principles of the Red Cross: commentary." (1979).

[15] European Union. “Humanitarian principles.” Last updated August 11, 2017. www.ec.europa.eu/echo/who/humanitarian-aid-and-civil-protection/humanitarian-principles_en

[16] Slim, Hugo. *Humanitarian ethics: A guide to the morality of aid in war and disaster*. Oxford University Press, 2015.

facilitate the pursuit of humanity and impartiality, as is seen later in this paper, this may not always be the case. In essence, this focus on independence and neutrality as means to other substantive ends indicates that while humanity and impartiality serve to determine what humanitarian actors do, neutrality and independence work to convince those who can block offers of aid to allow them to proceed instead.

What is so convincing about independence? The principle enforces a separation between an aid agency's decision-making and the agendas of others. This focus on separation from the agendas of others is the core of the definition of independence deployed in this paper. In a seminal volume on the question of humanitarian independence and manipulation, Antonio Donini connects independence to instrumentalisation: "[E]xamples include the blatant abuse and distortion of relief operations to achieve political objectives that are often antithetical to humanitarianism… [and] also include more subtle manipulations arising from the convergence of [aid agencies' and governments'] interests… around agendas related to globalisation, peace consolidation, nation building, human rights and justice."[17] Ed Schenkenberg van Mierop, executive director of a humanitarian think tank helpfully connects this with the notion of autonomy: "Independence is defined as being autonomous from the political, economic, military or other objectives that any actor may hold with regard to the area where humanitarian action is implemented… Independence implies institutional, political, financial and operational autonomy." [18] He follows, quoting the Fundamental Principles of the Red Cross: "The legitimacy of any humanitarian actor stands or falls on its capacity to withstand 'any interference, whether political, ideological or economic, capable of diverting it from the course of action laid down by the requirements of humanity, impartiality and neutrality'." Independence is jeopardised by the co-optation of humanitarian aid by governments or other actors who operate with their own agendas.

Co-optation might occur in two ways. First, autonomy may be lost through the surreptitious use of humanitarian organisations for ends other than those intended by their respective decision-makers. Part of persuading any relevant stakeholder that an offer of humanitarian assistance comes with no hidden agendas is convincing them that the organisation offering it has no ties to any other individual or group that may be pursuing other objectives. From the point of view of those with whom the humanitarian organisation is negotiating, it does not matter if they are aware of those ties or not. Independence is, therefore, linked to trust. The US government's clandestine appropriation of a humanitarian vaccination operation run by the NGO Save the Children in Pakistan in 2011 to collect blood samples to determine the location of Osama Bin Laden exemplifies this form of co-optation.[19] In this instance, Save the Children was not working autonomously, but was fundamentally co-opted into furthering a US government operation. During that operation at least, it was not independent of the

[17] Donini, Antonio, ed. *The golden fleece: manipulation and independence in humanitarian action*. Sterling, VA: Kumarian Press, 2012.

[18] van Mierop, Ed Schenkenberg. "Coming clean on neutrality and independence: The need to assess the application of humanitarian principles." *International Review of the Red Cross* 97, no. 897-898 (2015): 295-318.

[19] Bokhari, Farhan. "Pakistan expels Save the Children charity." *Financial Times*, June 12, 2015. www.ft.com/content/3dc496d6-10df-11e5-8413-00144feabdc0

US government. For Save the Children, trust in its assertion of independence was lost, and it was subsequently ejected from Pakistan. This form of lost independence is directly relevant to the challenges posed by technology discussed later in the paper.

Conversely, humanitarian organisations might overtly be involved in programmes that serve the strategy of another actor. Donini argues that, in practice, compromising on independence in this way has been the norm during the 150-year history of humanitarian institutions, drawing on case studies ranging from the Armenian genocide in 1915, to the Italian invasion of Abyssinia in 1935, through to state-building efforts in Somalia in the 1990s, and Afghanistan in the 2000s, as well as several more. Following Ian Smillie, "classic humanitarianism has not changed in its basic tenets, but it is applied by so many humanitarian organisations on such a sporadic and situational basis that it is difficult for manipulators to take it seriously. Or rather, it becomes easier for manipulators to ignore it."[20] The typology of motivations given for co-opting aid is illuminating: For states it includes geo-strategic advantage, counter-insurgency strategy, competition for markets/ resources, and military advantage; for non-state actors there is legitimacy to gain as well as political, economic, and again military advantage.[21]

These advantages do not only accrue to political organisations. Especially in the area of humanitarian innovation, the push for partnerships between governments or humanitarian organisations and the private sector is striking. Such collaborations are not a novelty to the 4IR; corporate social responsibility programmes pre-date this new set of technologies by several decades. However, the profit motives within the collaboration have arguably become much more central. The rise of so-called "informational capitalism," with data being labelled by some as "the new oil", is particularly relevant for this discussion of 4IR technologies.[22] Linnet Taylor and Dennis Broeders cite IBM's Project Lucy, based in Kenya, to support this case.[23] Project Lucy seeks to use artificial intelligence and big data analytics to deduce possible solutions to a range of issues in healthcare, education, agriculture, sanitation, and more. According to Taylor and Broeders, "It will involve feeding all the published economic and social data available from Sub-Saharan African countries into IBM's 'Watson' supercomputer, which will then data mine for answers to questions." The writers suggest the supercomputer may also have access to data that is not in the public domain. In their interviews with the people behind this innovation, the authors detect that "the standard for success is profitability,", quoting, for example, statements from the project's leader that, "I want my people to constantly ask themselves, 'Who's going to buy it?'", and from the chief data scientist that, "You have to be aware of the price point [for Project Lucy's findings]…You have to make the technology easily consumable."[24]

[20] Smillie, Ian. "The Emperor's Old Clothes." In A. Donini (ed) *The Golden Fleece: Independence and manipulation in humanitarian action.* Sterling, VA: Kumarian Press, 2012.

[21] ibid.

[22] Cohen, Julie E. "What privacy is for." *Harv. L. Rev.* 126 (2012): 1904.

[23] Taylor, Linnet, and Dennis Broeders. "In the name of Development: Power, profit and the datafication of the global South." *Geoforum* 64 (2015): 229-237.

[24] ibid.

In this way, profit-making agendas are also being connected to the decision-making of humanitarian groups.

As these interactions with private sector actors suggest co-optation is not necessarily resisted, although in other circumstances it may stem from ostensibly nobler motivations. Neo-humanitarianism was coined in the 1990s as a direct response to the perception that humanitarian aid, rather than alleviating suffering, was creating conditions to prolong it. This was attributed in large part to the unwillingness of humanitarian aid to endorse any larger agenda – which would evidently impact independence as understood in this paper – as well as its commitment to neutrality. Neo-humanitarians believe aid can and must serve development and peace-building in order to resolve the underlying causes of suffering and so end the cycle of its reproduction. For this reason, it is also known as "Wilsonian" humanitarianism after the liberal interventionist foreign policy espoused by Woodrow Wilson. In 1999, Mikael Barfod, a senior official at the European Community Humanitarian Office and early advocate of this line of thinking, argued "there is no way we can handle a situation without linking up with human rights issues, without linking up with development, to understand the real impact. We have to be part of the political process leading to peace, that is what we are really there for".[25] In her interpretation of Barfod's words, Fiona Fox wrote that "what characterises new humanitarianism is: the integration of human rights and peace building into the humanitarian orbit; the ending of the distinction between development and humanitarian relief; and the rejection of the principle of neutrality."[26] Such a position clearly comes at the expense of independence, with particularly important implications in places where the legitimacy or motives of the prevailing national government or foreign powers pushing development, human rights, or peacebuilding, are being questioned.

The result has been a vigorous and ongoing debate of the value and purpose of independence that goes to the core of what constitutes humanitarian action. Wilsonians have critiqued Dunantists for using the principle of independence to avoid engaging with the difficult questions surrounding causes of suffering, and thus facilitating its perpetuation. Meanwhile, soon after neo-humanitarianism gained traction, three critical concerns were raised about it.[27] The first concerned aid workers, who are unelected and generally remain unaccountable to the populations they affect, making what are fundamentally political decisions: "[t]hey are asked to reach verdicts on highly complex political crises, to decide which strategy would best deliver peace and stability and to predict the impact of humanitarian aid on the future development of a given conflict".[28] Of course, sometimes such responsibilities are inescapable. In the immediate aftermath of the 1994 Tutsi genocide in Rwanda, several refugee camps were infiltrated by armed groups involved in the mass killing.[29] This led to a

[25] Fox, Fiona. "New humanitarianism: does it provide a moral banner for the 21st century?" *Disasters* 25, no. 4 (2001): 275-289.
[26] ibid.
[27] ibid.
[28] ibid.
[29] Terry, Fiona. "The paradox of humanitarian action: Condemned to repeat." *London: Cornell* (2002).

split amongst aid agencies, conscious of the dilemma between refusing to distribute aid to civilians in desperate need or inadvertently supporting the ongoing activities of armed actors mixed up among them. While some agencies withdrew, others stayed. However, both decisions had obvious political implications.

Second, it introduces notions of deserving and undeserving aid recipients by motivating the withholding of assistance from populations affiliated with aggressors. Returning to the complexities of the Rwandan case, examples include Rwandan Hutus being denied needed assistance due to a perception of their collective guilt in the years following the Tutsi genocide.[30] In another instance, aiding Serb civilians was de-prioritised during and after the Balkans War, which included the Bosnian genocide by Serb forces.[31]

The third, and perhaps most controversial, is the elevation of human rights over basic needs that results, for example, in aid agencies suspending life-saving humanitarian programming following Taliban edicts restricting women's rights.[32] Here the discussion concerns the ethics of materially supporting an apparently objectionable ideology versus sacrificing the interests of people needing assistance here and now in the hope of facilitating change that will benefit others in the future. This underscores the intense moral dilemmas entangled with the notion of independence.

Stuart Gordon and Antonio Donini note the further criticism of Dunantist humanitarianism that, by eschewing any sort of transformational or emancipatory agenda, it can only focus on physical suffering, and so must dehumanise and diminish human beings to being only "bare life".[33] Accepting this, however, they argue that critiques of this classic humanitarianism have unfairly attributed a deontological rather than consequentialist interpretation of its principles, resulting in critics constructing neo-humanitarianism in reference to a strawman. In doing so, Gordon and Donini say they have produced a doctrine that sacrifices their ability to access many of those in need, and embraced their own co-optation into the security agendas generally of Western states. For them, the neo-humanitarians' willingness to be instrumentalised is responsible for emptying the concept of humanitarianism to the extent that "humanitarian war" is no longer an oxymoron. In their eyes, the divide is between a broader, deeper, more ambitious humanitarianism that promises broad empowerment but can only deliver to populations whose assistance serves Western agendas, and a humbler humanitarianism that is limited at best to maintaining bare life but in principle maintains the possibility of negotiating access to anyone in need of emergency assistance.

There are important implications to this divide. As Donini noted, many, perhaps even most, humanitarian groups continue conforming to this overall norm of co-optation. But some are still

[30] Thomson, Susan. "The darker side of transitional justice: the power dynamics behind Rwanda's gacaca courts." *Africa* 81, no. 3 (2011): 373-390.

[31] Boyd, Charles G. "Making peace with the guilty: The truth about Bosnia." *Foreign Affairs* (1995): 22-38.

[32] Vaux, Tony. *The selfish altruist: relief work in famine and war*. Routledge, 2013.

[33] Gordon, Stuart, and Antonio Donini. "Romancing principles and human rights: Are humanitarian principles salvageable?" *International Review of the Red Cross* 97, no. 897-898 (2015): 77-109.

working hard to protect and project their independence. Following the US-led invasion of Afghanistan in 2001, the ICRC went to great lengths to portray its independence from a state-building project that saw humanitarian aid provision as fundamental to its success. Nonetheless, in 2003, Ricardo Munguia, one of its delegates, was murdered by Taliban fighters, who presumed he was part of the state-building effort they sought to resist. Underscoring its operational role of the principle in providing humanitarian assistance, the questioning of the ICRC's independence forced the organisation to drastically reduce its operations for people living in areas under Taliban control. However, this reduction included carefully identified activities, building gradually from work in detention centres to support emergency healthcare services in Helmand and Kandahar, ultimately demonstrating its independence to the satisfaction of opposition groups, and thus gaining their support.[34] Meanwhile, Médecins Sans Frontières (MSF), unlike the ICRC, relies on donations from the public to support its operations. Nonetheless, it refuses money from governments with interests in the areas they work, and also rejects funding from any other entity that has demonstrable concerns in a given context in which they are running an operation, such as extractive industries.[35]

While a more detailed account is beyond the scope of this paper, a further important cleavage falls between European/ Western discussions and the conceptions of humanitarianism percolating in the rest of the world. These are argued often to reject discussions of classic humanitarian principles as rooted in imperial ideology.[36] In China, it is argued, efforts to "liberate" the concept of humanitarianism from the bourgeoisie – considered synonymous with Western imperialism – using Communist Party principles such as "people-oriented" governance and Confucian scholarship of the notion of benevolence and hierarchical duties of charity, makes humanitarianism part of the conceptualisation of the responsible exercise of sovereignty.[37] This explicit connection of humanitarianism and state presents an alternative position in which the independence of humanitarian organisations is considered neither desirable nor possible.[38] While scholarship on Southeast Asian views on humanitarianism is more limited, a similarly statist result is likely to stem from the prioritisation given to non-intervention, again argued to stem from the colonial experience, alongside the categorisation of humanitarianism as part of non-traditional security (NTS). In Southeast Asia, the concept of NTS has led to a re-articulation of security to include elements of human security, introducing humanitarian concern into the securitisation debate.[39] Nevertheless, state interests remain part of the NTS equation, which again has implications on the possibility of truly independent humanitarian action. With experimentation of 4IR technologies in humanitarian emergencies occurring in these regions as

[34] Terry, Fiona. "The International Committee of the Red Cross in Afghanistan: reasserting the neutrality of humanitarian action." *International Review of the Red Cross* 93, no. 881 (2011): 173-188.

[35] "International Financial Report 2016." *Medecins Sans Frontieres* (2017), edited by Marisol Gajardo, Gabriel Lebailly, and Ricardo Rubio. www.msf.org/sites/msf.org/files/msf_financial_report_2016_final.pdf

[36] Yeophantong, Pichamon. *Understanding humanitarian action in East and Southeast Asia: A historical perspective*. Humanitarian Policy Group, 2014.

[37] ibid.

[38] Gordon, Stuart, and Antonio Donini. "Romancing principles and human rights: Are humanitarian principles salvageable?" *International Review of the Red Cross* 97, no. 897-898 (2015): 77-109.

[39] Emmers, Ralf, and Mely Caballero-Anthony. "Understanding the dynamics of securitizing non-traditional security." In *Non-Traditional Security in Asia*, pp. 13-24. Routledge, 2017.

well, such differences over the nature of humanitarianism will inevitably produce different and important implications on the critical discourse around humanitarian innovation.

In sum, independence is under serious challenge both in humanitarian practice and in principle. These ongoing contestations represent an important discursive context in which the challenges that 4IR technologies pose for humanitarian independence must be understood. Let us now discuss those technologies in order to draw this out explicitly.

# New Technologies and Independence: A Question of Capability and Vulnerability

In its *Handbook on Data Protection in Humanitarian Action*, which aims to give practical and legal guidance to humanitarian groups handling data, the ICRC raises three instances in which data management prompts concern about independence.[40] The first is when humanitarian organisations are requested to share data with state authorities; the second is when they consider sharing data with third parties, such as other NGOs or for-profit actors; and the third is when unintended third parties gain access to that data. The first two options relate to deliberate choices made by humanitarian groups and so are particularly apt for the consideration and policy guidance provided in the handbook. However, the third opens up a much larger field of structural concerns relating to the motivations for third parties to seek such unintended access to data held by humanitarians, and the means by which they gain that access. This requires deeper examination, particularly through the lens of the 4IR.

Fundamentally, the crossing of physical and biological domains with the cyber one – the key characteristic of the 4IR – both raises the motivations for accessing data held by humanitarian organisations, and facilitates that access. Aid organisations are already present in politically delicate areas and collecting information there that political and military entities would consider sensitive, and in which corporations might see profit, as part of their humanitarian objectives. Indeed, quite apart from the 4IR, they have historically been targeted by state and non-state actors seeking to gather intelligence with which to further their own respective military or political strategies. Prominent examples include North Korea, where the US is reported to have co-opted missionaries engaged in humanitarian work,[41] and East Timor, where Australia reportedly used aid workers engaged in construction for intelligence purposes.[42]

The extent of 4IR technological use strengthens this pre-existing motivation by radically expanding the surveillance and intelligence production capabilities of humanitarian groups. Subsequent digitised data is more easily shared and replicated, and humanitarian operations' exposure to global communications networks increases exponentially; in principle at least, 4IR technologies allow

[40] Kuner, Christopher Barth, and Massimo Marelli. "Handbook on data protection in humanitarian action." (2017).
[41] Cole, Matthew. "The Pentagon's Missionary Spies." *The Intercept*, October 26, 2015. www.theintercept.com/2015/10/26/pentagon-missionary-spies-christian-ngo-front-for-north-korea-espionage/
[42] McGrath, Kim. *Crossing the Line: Australia's Secret History in the Timor Sea*. Black Inc., 2017.

everything in the physical world to be connected to, and communicate with, everything else. The ensuing cybernetic outcome already raises interesting questions about the very separateness of aid organisations from other entities. But leaving this aside, the underlying order through which humanitarian organisations manage to negotiate access to places where populations in need can reach them – which often relies on the principle of independence in particular – means that 4IR technologies pose particular concerns for them that do not apply in corresponding government or private sectors.

Recalling that independence is a function of autonomy, the integration of humanitarian operations into global information networks is relevant as it presents more opportunity to other cyberspace inhabitants to access data collected for those operations and employ it for their own agendas. This is comparable to the so-called "capability/ vulnerability paradox" discussed in literature on cybersecurity of military systems[43] and smart cities.[44] In essence, as organisations insert a greater proportion of their operational management into cyberspace for gains in efficiency and effectiveness, they expose those operations to a commensurately increased threat of compromise through cyber-attack. This paradox is arguably starkest in military settings, where the connection of defensive and offensive real-world systems within cyberspace allows for an intensive level of coordination between component parts of those arrays, and of automation of the resulting meta-system, delivering substantial gains in effectiveness. However, this increased presence in cyberspace expands the attack surface available for opposition cyber weapons to target too, and the connectivity of these weapons systems means that any successful cyberattack on one component could compromise the entire defensive or offensive array. As formidable as a cyber-connected, fully integrated and coordinated weapons system may be, the very means through which it is created introduces new vulnerabilities that potentially allow for it to be fully compromised.

Short of completely disabling a system, greater cyber capabilities also facilitate unauthorised access to data while leaving the overall system intact, as well as data's negligent loss. This represents a second category of vulnerability. There are many examples of both these possibilities. In 2016, the US Democratic National Committee computers were infamously hacked, and tens of thousands of emails were stolen.[45] The same year, US Office of Personnel Management data was breached for a second time, with attackers targeting personal information of military and intelligence personnel applying for security clearance.[46] In 2016, the Philippines' Commission on Elections' website was hacked and its entire database stolen.[47] Beyond theft of stored data, if a system has sensory

[43] Schneider, Jacquelyn. *Digitally-enabled Warfare: The Capability-vulnerability Paradox*. Center for a New American Security, 2016.

[44] Kitchin, Rob, and Martin Dodge. "The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention." *Journal of Urban Technology* (2017): 1-19.

[45] Sanger, David E., and Nick Corasaniti. "D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump." *New York Times*, June 14, 2016. www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html

[46] Koerner, Brendan I. "Inside the cyberattack that shocked the us government." *Wired. com* (2016): 1.

[47] Temperton, James. "The Philippines election hack is 'freaking huge'." *Wired*, April 14, 2016. www.wired.co.uk/article/philippines-data-breach-fingerprint-data

capabilities of its own, then its perception of the real world around it is also vulnerable. In a particularly striking demonstration of this, Insecam.org streams the feeds of thousands of compromised security cameras from around the world live on the internet.[48]

How do these capabilities and vulnerabilities manifest in humanitarian operations? Surveillance and intelligence producing capabilities in particular have been strengthened. Unmanned aerial vehicles (UAVs) are now a regular feature of data gathering. They were used following the 2010 earthquake in Haiti, and the 2013 Typhoon Haiyan in the Philippines.[49] For instance, the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo, is using UAVs for reconnaissance and data-gathering, and offering those capabilities to humanitarian organisations working in the area.[50] If used appropriately, the mapping resolutions achievable through this technology, which can be coupled with various sensory equipment and software programmable for different information-gathering tasks for operational planning and deployment, can give a near real-time picture of an operating environment that is of clear strategic benefit to humanitarians as well as any state or non-state actor interested in the area.

The organisation Artificial Intelligence for Disaster Response (AIDR) is using artificial intelligence on social media to provide real-time contextual understanding in a different way. AIDR takes the vast quantity of publicly available social media posts made for areas of interest and – using a combination of human and artificial intelligence – categorises them in ways considered relevant for humanitarian groups to populate maps, or any other interface that may be deemed useful.[51] The algorithm can work similarly with text and image-based posts, indexing them in ways that facilitate subsequent analysis.

High levels of mobile phone penetration, particularly third and fourth generation mobile phones, result in several active and passive data collection opportunities. The World Food Programme used text messaging, interactive-voice recording and live calls in the Democratic Republic of Congo, Somalia, and Ebola-affected countries in West Africa during the 2013 outbreak, to gather data relating to food security.[52] Following the Haiti earthquake and the subsequent cholera outbreak, Swedish non-profit organisation Flowminder trialled the use of call detail records to track population displacement.[53] They did the same in the aftermath of the Nepal earthquakes in 2015, using data to identify, quantify and locate population outflows from Kathmandu to surrounding districts. Since 2015, work has been done

[48] Cox, J. "This Website Streams Camera Footage from Users Who Didn't Change Their Password. Motherboard, Oct 31st." (2014).

[49] "Drones for Disaster Response and Relief Operations." *American Red Cross and Measure* (2015): www.issuelab.org/resources/21683/21683.pdf

[50] Gilman, Daniel. *Unmanned aerial vehicles in humanitarian response*. UN, 2014.

[51] GitHub. "AIDR Overview." Last modified October 24, 2016. www.github.com/qcri-social/AIDR/wiki/AIDR-Overview

[52] Obrecht, Alice, and Alexandra T. Warner. "More than just luck: Innovation in humanitarian action." *HIF/ALNAP Study* (2016).

[53] Wilson, R., zu Erbach-Schoenberg, E., Albert, M., Power, D., Tudge, S., Gonzalez, M., Guthrie, S., Chamberlain, H., Brooks, C., Hughes, C. and Pitonakova, L., 2016. Rapid and near real-time assessments of population displacement using mobile phone data following disasters: the 2015 Nepal Earthquake. *PLoS currents*, *8*.

processing cellular data using artificial intelligence to identify further characteristics about users, including gender, age, and socio-economic status.[54] These data, which correlate closely with overall disaster vulnerability, are typically not available for pre-paid mobile phones, which make up the majority of mobile phone connections in the developing world. Researchers at Imperial College London have developed an algorithm that can learn about typical mobile phone usage conventions in different social contexts to identify these traits from a user's habits, thus facilitating the prioritisation of vulnerable groups such as women and children in the planning of emergency response, and allocation of resources in areas where such demographic data is unavailable or unreliable. Such data relating to the situation and movement of people is also of clear strategic benefit not just to humanitarians, but any actor vying for influence or otherwise operating in that location.

The growing availability of smartphones and tablets has increased the speed, quantity, and quality of population level data collection and processing. In Pakistan, the Internally Displaced Person Assessment and Profiling project has used data software to make the number and situation of those displaced people living outside of camps more visible to humanitarian and government policymakers.[55] It comprises a questionnaire specifically designed to identify issues related to food, child protection needs, and cash shortages, all contained within software downloaded to a smart phone. This allows complex analysis of insecurity crossing several variables (for example, female-headed households with more than four children, one or more of whom have a chronic disease), and the creation of individualised profiles categorised according to vulnerability and monitored in case of deterioration.

The UN has trialled collecting various pieces of biometric data from refugees in Afghanistan and in Lebanon in order to better monitor its distributions of material aid and repatriation processes.[56] In this particular instance, the potential intelligence interest in this data is underscored by the behaviour of refugees themselves, some of whom are recorded as having burnt off their fingertips in order to circumvent the technology, or as deciding to forego registration and hence aid, entirely due to their fears about how the information collected might be subsequently used against them.[57]

Social network analysis is another interesting use of software for data processing. It focuses on the nature and significance of the relationships between actors, rather than the actors themselves, helping understand the political context in which humanitarian operations are run.[58] Here a

[54] Jahani, Eaman, Pål Sundsøy, Johannes Bjelland, Linus Bengtsson, and Yves-Alexandre de Montjoye. "Improving official statistics in emerging markets using machine learning and mobile phone data." *EPJ Data Science* 6, no. 1 (2017): 3.

[55] Vinck, Patrick, ed. *World Disasters Report 2013: Focus on Technology and the Future of Humanitarian Intervention*. International Federation of Red Cross and Red Crescent Societies, 2013.

[56] "Report of the International Conference on the Solutions Strategy for Afghan Refugees to support Voluntary Repatriation, Sustainable Reintegration and Assistance to Host Countries." UNHCR, Geneva, Switzerland, May 2-3, 2012.

[57] Jacobsen, Katja Lindskov. *The politics of humanitarian technology: good intentions, unintended consequences and insecurity*. Routledge, 2015.

[58] Zwitter, Andrej. *Humanitarian Intelligence: A Practitioner's Guide to Crisis Analysis and Project Design*. Rowman & Littlefield, 2016.

humanitarian organisation inputs various data points it has gathered about key local actors, many of which will come from direct meetings that are only possible through the privileged presence it has in that area. This is especially useful in unstable contexts in which power brokers often exist in an element of obscurity.

Finally, IoT technology has been successfully trialled in several humanitarian contexts. The level of material surveillance it allows has helped to manage the cold chain, which keeps temperature-sensitive pharmaceuticals in the correct temperature band to maintain their effectiveness.[59] This can be particularly difficult in remote settings or areas where power supplies are disrupted, which are often precisely where humanitarian organisations are working. The temperatures to which drugs are exposed are automatically tracked, and alerts sent if those temperatures exceed those that the drug can tolerate. This data is stored on the Cloud for analysis to monitor the overall performance of refrigerator units. IoT is also being trialled in humanitarian supply management since it allows the precise tracking of items through the supply chain, increasing the reliability of delivery and the flexibility to reroute supplies if necessary.[60] [61] Items are given a unique tracking address, to which different data regarding freight type, quantity, location and state, can be attached. The addresses can then be used to programme and easily re-programme specific instructions for distribution. This produces a functional map of all the supply chain’s moving parts that can be analysed in order to identify ways to make the process more efficient.

IoT trials are ongoing with medical devices that allow remote monitoring and control of any medical device hooked up to a patient. A dip in their vital signs prompts an alert to the patient, allowing them to take more control of the situation and take action. Alternatively, it can alert medical staff nearby or, potentially, can prompt the automatic release of a drug to counteract the situation. This possibility of remote monitoring has been particularly beneficial in managing infectious diseases, and this system has been trialled with success by USAID during the Ebola outbreak in West Africa,[62] In this case, it allowed for a reduction of the time that health workers spend in personal protective equipment in highly infectious areas within Ebola treatment centres, and quicker identification of the moment patients  become symptomatic, which is the moment they become infectious and require isolation. The level of monitoring facilitated by Internet connections is also generating interest for improving water purification efficiency,[63] and even tracking vehicles in humanitarian settings.[64]

[59] Biggs, P., J. Garrity, C. LaSalle, A. Polomska, and R. Pepper. "Harnessing the Internet of Things for global development." *International Telecommunication Union* (2016).

[60] Oloruntoba, Richard, and Richard Gray. "Humanitarian aid: an agile supply chain?" *Supply Chain Management: an international journal* 11, no. 2 (2006): 115-120.

[61] Yang, Lili, Shuang-Hua Yang, and L. Plotnick. "How the internet of things technology enhances emergency response operations." *Technological Forecasting and Social Change* 80, no. 9 (2013): 1854-1867.

[62] Biggs, P., J. Garrity, C. LaSalle, A. Polomska, and R. Pepper. "Harnessing the Internet of Things for global development." *International Telecommunication Union* (2016).

[63] ibid.

[64] Yang, Huanjia, Lili Yang, and Shuang-Hua Yang. "Hybrid Zigbee RFID sensor network for humanitarian logistics centre management." *Journal of Network and Computer Applications*34, no. 3 (2011): 938-948.

# Using Cyber-space and Losing Strategically Valuable Intelligence

These extensive capabilities made possible through 4IR technologies come with the same vulnerabilities as noted in military and urban development settings – both cataclysmic operational compromise and unauthorised data access. The possibility of cyberattacks disabling efforts to provide humanitarian assistance is of increasing interest to international humanitarian lawyers. Within that literature there is broad consensus that cyberattacks on hardware that cripple the provision of humanitarian aid are sufficiently analogous to a kinetic military attack so as to constitute a war crime under existing international humanitarian law (IHL).[65] [66] [67] Similarly, Rule 86 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* which, while a non-binding study, is the most comprehensive assessment of the rules governing cyber warfare, states that "cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance."[68] Of course, prohibition has not stopped conventional kinetic attacks on humanitarian installations in recent years when such attacks have been in the strategic interest of their perpetrators, demonstrating limits to the protection such global norms offer. Though potentially far more serious in the immediate term, these cyberattacks have fewer implications on the principle of independence. It is the second vulnerability regarding data access that is more pertinent here.

There are several examples of cyber-enabled loss of humanitarian data both through negligence and through hostile attacks. In late 2017, an audit of the World Food Programme's SCOPE data management system, ultimately intended to handle personal details of the more than 80 million people receiving food assistance from the agency, found several crucial safeguards missing or unimplemented,[69] leading one data specialist to label this situation "an accident waiting to happen".[70] This included unnecessary data being collected, including some of an evidently sensitive nature such as "religion", the retention of personal data of those no longer receiving assistance, inadequate consent and insecure and unregulated sharing of data with third parties. In another worrying instance, a data tracking platform created by private company Red Rose and used by Catholic Relief Services gave unauthorised access to names, photographs, family details, PIN numbers, and map coordinates of more than 8,000 families receiving assistance from the NGO, ostensibly due to a password management error.[71] Commenting on this incident, the team at the Harvard Humanitarian Initiative

[65] Dörmann, Knut. "Applicability of the Additional Protocols to computer network attacks." In *International Expert Conference on Computer Network Attacks and the Applicability of IHL, Stockholm*, p. 3. 2004.

[66] Melzer, Nils. *Cyberwarfare and international law*. United Nations Institute for Disarmament Research, 2011.

[67] Dinniss, Heather Harrison. *Cyber warfare and the laws of war*. Vol. 92. Cambridge University Press, 2012.

[68] Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

[69] "Internal Audit of Beneficiary Management." *World Food Programme* (2017): www.docs.wfp.org/api/documents/WFP-0000040084/download/?_ga=2.43869413.1326768420.1516256388-1682848339.1511261484

[70] Parker, Ben. "Audit exposes UN food agency's poor data-handling." *IRIN News*, January 18, 2018. www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling

[71] Raymond, Nathaniel A., Scarnecchia, Daniel P., and Stuart R. Campo. "Humanitarian data breaches: the real scandal is our collective inaction." *IRIN News*, December 8, 2017. www.irinnews.org/opinion/2017/12/08/humanitarian-data-breaches-real-scandal-our-collective-inaction

researching ethics and standards relating to the use of data in humanitarian settings notes that "the fact of the matter is that critical failures and breaches of information systems are an open secret in our sector," although tangible evidence and discussion of this is limited "due to fears by individuals and organisations of the financial and reputational repercussions of publicly documenting them".[72] This represents a broad consensus that data leaks are both common and vastly underreported in the sector.

Substantial breaches are not surprising. The United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) notes that the volumes of data now being handled by humanitarian groups are "often outstripping their capacity to analyse risks and sensitivities".[73] Those guidance documents that do exist "do not address many emerging issues, such as privacy laws, safe handling of metadata, standards for anonymization, assessments of cyber security, or the role of technology providers".[74] In a particularly damning assessment, Kristin Bergtora Sandvik, of the Peace Research Institute Oslo notes that "poor information management – including inadequate policies and insufficient training – risks turning humanitarians into threat actors in cyberspace."[75] To the extent that poorly managed data is inadvertently leaked or otherwise made available to others, autonomy over that data is undermined and, by extension, independence compromised.

Notable efforts are being made to rectify this, including moves towards developing a theory of harm for discussions of data security,[76] and the conception of a rights-based approach to managing digitised data about vulnerable groups in humanitarian settings.[77] The General Data Protection Regulation recently promulgated by the European Union also brings significant pressure on Europe-based agencies to improve the way they collect and process data, with provisions included to return some level of control to the subject of that data.[78] These are positive developments. However, even in the most optimistic improved data hygiene scenario, the capability-vulnerability paradox underscores the extent to which cyber-based technologies create a logic that encourages deliberate efforts to access data held by humanitarian groups. Daniel Gilman of UN OCHA points out that "systematic targeting of humanitarian information systems and the people who use them by groups linked to

[72] ibid.

[73] Gilman, Daniel. *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies*. United Nations Office for the Coordination of Humanitarian Affairs, 2014.

[74] ibid.

[75] Sandvik, Kristin Bergtora. "The humanitarian cyberspace: shrinking space or an expanding frontier?" *Third World Quarterly* 37, no. 1 (2016): 17-32.

[76] Sandvik, Kristin, and Nathaniel A. Raymond. "Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response." (2017).

[77] Greenwood, Faine, Howarth, Caitlin, Poole, Danielle Escudero, Raymond, Nathaniel A., and Daniel P. Scarnecchia. "The Signal Code: A Human Rights Approach to Information During Crisis." *Harvard Humanitarian Initiative* (2017): www.hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis

[78] Regulation, General Data Protection. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46." *Official Journal of the European Union (OJ)* 59 (2016): 1-88.

military and security actors pose a direct challenge to the humanitarian space."[79] This means improved data management may not be sufficient to maintain autonomy over the uses to which data is put.

There is mounting evidence of systematic targeting of humanitarian agencies by cyber attackers for data they possess. The European Interagency Security Forum noted several media reports of both the British and Chinese governments using cyber-based methods to garner information from Médecins du Monde, United Nations Children's Emergency Fund and World Health Organization.[80] Files leaked by Edward Snowden, a former contractor working for the National Security Agency in the US, detail comparable attacks again by the British and also the US governments on humanitarian groups.[81] The Satellite Sentinel Project, which seeks to operate as an early warning system for outbreaks of violence, has been targeted by groups seeking access to its satellite feed.[82] Several attacks have been recorded in Syria against NGOs, activists, and civil society organisations.[83] These include the embedding of malicious links masquerading as articles on certain websites known as "watering holes", where the personnel of targeted organisations are known to visit to gather their own open-source information. Spear-fishing, where NGO staff receive emails from trusted accounts containing malicious links presented as information they have either requested or in which they are known to be interested, is also common. Finally, in one research paper, as many as 80,000 "hostile events" were recorded on a WiFi network for displaced peoples in Greece per week.[84]

Apart from aggressive targeting, there is evidence that organisations with intelligence links may be marketing data aggregation and analysis tools to humanitarian groups as a means to get access to that data.[85] Palantir, a company with acknowledged ties to the Central Intelligence Agency, has developed software capable of aggregating data from both open and closed sources held by a humanitarian organisation and presenting it within a single interrogable tool. Those in the industry reportedly believe that Palantir is not alone in simultaneously providing services to humanitarian organisations and having links with the intelligence community.[86]

[79] Gilman, Daniel. *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies*. United Nations Office for the Coordination of Humanitarian Affairs, 2014.

[80] Byrne, Rory. "Trends in intelligence gathering by governments." In *Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF) Google Scholar*. 2016.

[81] Ball, James, and Nick Hopkins. "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief." *The Guardian*20 (2013).

[82] Gilman, Daniel. "Cyber-Warfare and Humanitarian Space." In *Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF)*. 2014.

[83] Byrne, Rory. "Trends in intelligence gathering by governments." In *Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF) Google Scholar*. 2016.

[84] Maitland, Carleen, and Rakesh Bharania. "Balancing Security and Other Requirements in Hastily Formed Networks: The Case of the Syrian Refugee Response." (2017).

[85] Anyadike, Obi. "Spies Sans Frontières? How CIA-linked Palantir is gaining ground in the aid industry (and why some humanitarians are worried)." (2016).

[86] ibid.

In contrast to the apparent consensus within IHL regarding the prohibition of attacks that affect the real world ability of humanitarians to provide aid noted above, IHL currently offers little in way of defence against cyber intrusions that extract data without reducing an organisation's operational capacity. While in the past accessing detailed data collected by humanitarians would require the physical penetration of their compounds to take documents (an act that is prohibited by IHL) – technology has enabled such unauthorised access without the actual violation of the agencies' premises, meaning such an action remains IHL-compliant. Indeed, some suggest IHL may even *create* a "duty to hack" humanitarian organisations.[87] IHL calls on belligerents to use the minimum level of military force required to achieve their strategic objectives and thus limit the risk of harming non-combatants. This is part of IHL's principle of proportionality requiring parties to a conflict to gather as much intelligence as they can in order to make their military actions as surgical as possible to limit suffering and loss of life. If information held by humanitarian groups operating in the theatre of war can assist in that regard—and new capabilities outlined above are making this increasingly likely—then that information must presumably be accessed. This is the tension between 4IR technologies and the prevailing humanitarian regime at its starkest, taking previously compatible rules of IHL and pushing them to undermine each other. While the principle of independence requires humanitarian groups to avoid becoming instruments of government policy, new technologies are interacting with existing IHL provisions to press governments into making humanitarian agencies into appendages in support of their activities.

IHL could be reconstrued to prohibit even this type of cyber intrusion on humanitarian groups that do not result in damage analogous to a kinetic attack. There are calls to this effect. Daniel Gilman calls for cyber intrusions for the purpose of data-theft to be made explicitly an IHL violation. In this regard, we should carefully watch discussions on the creation of a humanitarian cyberspace, potentially with a digital Geneva Convention. However, even if such agreements were reached, they could only rely on the normative power of such a provision to influence state behaviour. This would represent important progress, but is unlikely to be sufficient to discourage such targeting of humanitarian groups. The strategic logic behind hacking humanitarian information systems would remain. Indeed, several writers point out that the difficulty in attributing cyberattacks likely means such a prohibition would have very limited impact on state behaviour.[88] [89] One legal scholar notes that "the lack of accountability offers an incentive for states to engage in prohibited cyberattacks. The structure of the Internet makes detection and attribution unlikely".[90] As such, regardless of any norms to the contrary, if an attack on humanitarian information systems brings strategic advantage, it is likely that states, or indeed any other actor, will conduct it. This again reminds us of the difficulty in stopping the ongoing bombings of hospitals in Syria and Yemen when such actions serve a military strategic interest.

[87] Hollis, Duncan B. "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" In J. D. Ohlin, K. Govern, and C. Finkelstein (eds) *Cyberwar: Law and Ethics for Virtual Conflicts*. (2014).

[88] Lin, Herbert. "Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94, no. 886 (2012): 515-531.

[89] Kelsey, Jeffrey TG. "Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare." *Michigan Law Review* (2008): 1427-1451.

[90] ibid.

With limited protection furnished by global norms, autonomy over the use of data humanitarians collect hinges on aid organisations' capacity to protect data from unauthorised access. Two arguments underscore the difficulty they face achieving this. First, the level of cybersecurity required to achieve this is likely to be prohibitively expensive. Several high profile data thefts, such as the twin breaches of the US Office of Personnel Management targeting personal information of military and intelligence personnel applying for security clearance noted above, show that even the world's most powerful and well-resourced states struggle to keep their data secure.

Second, the level of data protection required by the principle of independence may simply not be possible in an era of rapidly evolving planetary scale networking. The World Economic Forum considers the substantive interdependence of all entities in cyberspace a foundational assumption for its discussions of cybersecurity. This is based on its position that connectivity now underwrites the normal functioning of society.[91] In a discussion on cybersecurity of critical state infrastructure, Dave Clemente of Chatham House argues along similar lines, noting that the increasing penetration of cyber space into the political and economic sectors of societies make it more and more difficult to isolate them from each other.[92] To the extent this happens in the humanitarian sector, the result is presumably the same.

In this hyper-connected space, several elements combine to make resistance to a cyber intrusion extremely difficult. The complexity and constant flux of network topographies and topologies already challenge the capacity of humans to visualise, comprehend and thus counter. This, combined with the millisecond speeds at which attacks occur, and the high noise to signal ratio in monitoring mechanisms that make even perceiving an attack difficult, move cyber defence beyond human capability. While automated defences can meet these challenges, they have their own shortcomings. For example, neither can they handle situations for which they are not programmed, nor can they deal with novelty. With the US air force predicting that by 2025 there will be 200 million new malware signatures a year, this is a significant shortcoming.[93]

This does not make cybersecurity a futile endeavour; however, it has fundamentally shifted its conceptualisation with particular relevance to humanitarian independence. There is widespread acceptance that connectivity has reached a level at which complete local network integrity has become unattainable. Correspondingly, analysts now situate prevention within a broader approach of "cyber resilience" that accepts the ever-present possibility of unauthorised access and strategises

[91] "Partnering for Cyber Resilience." *World Economic Forum* (2012): www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

[92] Clemente, Dave. *Cyber security and global interdependence: what is critical?* Chatham House, Royal Institute of International Affairs, 2013.

[93] Maybury, Mark T. *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025*. Technical Report No. AF/ST TR 12-01). Retrieved from http://www. defenseinnovationmarketplace. mil/resources/cyber/cybervisi on2025. pdf, 2012.

accordingly.[94] [95] This reframes the issue as a probabilistic one; it is about reducing the chance of a breach to an organisationally acceptable level and preparing contingency plans to minimise the damage done should data be lost.

Fundamentally, accepting the possibility of losing data as a price to pay for the benefits of linking to the hyper-connected world resulting from the 4IR is not in itself anathema to core operational models of business or states. Governments and private corporations can continue to function much like they always have, while still openly acknowledging they may lose data. For the private sector, in principle risk needs only to be mitigated to the satisfaction of consumers. Similarly, in the governing sector, state institutions must only placate the concerns of those constituencies within their respective populations with the power to challenge them and their policies. The experience of making policy for and constructing "smart cities" suggests that, both as consumers and as citizens, people continue to value speed and convenience over security.[96] The organisationally acceptable level of risk is actually quite high. Seen through the lens of the capability-vulnerability paradox, this probabilistic view means organisations can frame their reflections on inserting themselves deeper into cyberspace in relatively straightforward terms of costs and benefits to their core functions and services.[97]

This cost-benefit calculation cannot apply in humanitarian contexts. The costs in question fall not on aid organisations but on actors with whom humanitarians must negotiate their presence in a given territory. Meanwhile the benefits fall not on those negotiating actors but instead on people caught in areas under their control. Due to this distribution of risks and benefits, those negotiating actors are unlikely to put speed and convenience over security in the way consumers and citizens have. Meanwhile, those receiving the benefits of humanitarian operations are, by definition, largely disempowered and unable to exert influence to the contrary. By accepting the ever-present possibility of losing data as part of their ordinary operational functioning – a situation that has been argued above to exist exclusively due to the insertion into cyberspace entailed by adopting 4IR technologies – humanitarians also accept the loss of autonomy over that data. This compromise on independence raises risks for actors with whom they negotiate access without providing any benefits with the potential to counter-balance the risk. As such, to the extent that humanitarian groups rely on perceptions of their independence to negotiate access, the organisationally acceptable level of cyber-intrusion risk must be close to zero. In passing, this logic would result in the same conclusion to the "do no harm" principle. Accepting any level of risk of losing data means the duty to do no harm can never be satisfied. The best that can be achieved is to maximise benefit while minimising harm – a very different ethical proposition.

[94] Nicholas, Paul. "Cybersecurity and cyber-resilience – Equally important but different." *Microsoft*, November 3, 2016. www.cloudblogs.microsoft.com/microsoftsecure/2016/11/03/cybersecurity-and-cyber-resilience-equally-important-but-different/

[95] Brasso, B. "Cyber attacks against critical infrastructure are no longer just theories." *online], Fire-Eye, https://www. fireeye. com/blog/executive-perspective/2016/04/cyber_attacks_agains. html. EY. (2014)"Achieving Resilience in the Cyber Ecosystem* (2016).

[96] Kitchin, Rob, and Martin Dodge. "The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention." *Journal of Urban Technology* (2017): 1-19.

[97] ibid.

For non-Dunantist groups this situation is perhaps less problematic. Their broader goals of peace-building, human rights, development and/ or state-building, or simply furthering the agendas of the respective states from which they hail, already preclude the possibility of working in areas controlled by groups resisting those political agendas, both due to the strategic logic of those objectives and the tactical reality that those groups would not grant such access in the first place. Any strategically valuable information they leak from places they are permitted to work would undermine only the interests of actors pursuing aims to which they are already connected, meaning the ever-present need to demonstrate distance from opposition agendas is not there. While this might raise questions on competence, which are certainly not without operational implications, the underlying trust on which their access is granted stems from elsewhere and so is unaffected.

This is not the case for Dunantist agencies, for whom this implicit trust born of agenda conformity does not, by definition, exist. These challenges to independence may consequently make it harder to convince those with the power to block, to instead allow aid agencies into areas they control. Why would a political or military leader allow a humanitarian organisation to operate in his or her territory if its leaders cannot guarantee they will not become a vector for his or her opponents to access strategically valuable intelligence? From his or her point of view, whether deliberately or otherwise, such an agency is unable to exercise sufficient decision-making autonomy over the data it collects and the information it produces. Practically speaking, this means that the agency is not independent. Comparable to the Save the Children/ US government example cited earlier, by facilitating the production of strategic intelligence while simultaneously increasing its vulnerability to unauthorised access, 4IR technology is increasing the likelihood of humanitarian organisations unwittingly functioning as appendages of other actors pursuing agendas that diverge from the humanitarian objectives for which data was originally collected. This could potentially run contrary to the objectives of those with whom they must negotiate access to populations in need.

# Conclusion

Two related trends stemming from the introduction of 4IR technologies into humanitarian operations are undermining humanitarian principles by creating a capability/ vulnerability paradox. While there are evident implications on neutrality and the duty to do no harm, this paper has focused on the challenges posed to humanitarian independence, which is often central to negotiating access to people in need. First, the improved quality of data gathering and information processing increases the likelihood that aid agencies are producing strategically valuable intelligence. Second, the central role of cyber in 4IR technology makes that information more vulnerable to unauthorised access, meaning it is easier for other actors to appropriate humanitarians as appendages to their own agendas.

Independence is a key contention between Dunantist and non-Dunantist humanitarians, irrespective of the latter being Wilsonian or hailing from non-Western settings. It is the difference between performing humanitarian action to further state or principled agendas through which it is hoped that the causes of suffering will be addressed at the expense of providing aid to all who need it, or instead giving aid based on need alone while eschewing concerns about justice, development, peace, and the general causes of their suffering. This challenge to independence has important operational effects for Dunantist organisations as well as material implications within this principled discussion.

Operationally, all else being equal, humanitarians must seek to maximise their efficiency and effectiveness in order to meet more needs of more people. Possibilities for using new technology to this end must be explored. However, independence is an instrumental value – precisely in that it assists the negotiation of access to areas where humanitarian aid is needed. Once the perception of independence is lost in the eyes of negotiating partners – whether for reasons of data loss or anything else – access vanishes. This represents a potential trade-off of access for effectiveness. On the one hand, 4IR technologies are of instrumental value – that is, they will presumably result in better outcomes for the individuals that humanitarians seek to assist. On the other hand, they jeopardise the instrumental value of independence, with any loss of trust potentially moving people in need out of reach of assistance. This trade-off is reminiscent of a call within the cyber security debate regarding smart cities to use airgaps – physical separations within an otherwise connected system – strategically to improve information security, even at the expense of gains in speed, efficiency or effectiveness.[98]

These reflections also introduce a material imbalance into this dispute over the independence principle. Groups that do not consider independence important are freer to insert themselves deeper into cyber space in the pursuit of operational gains. The 4IR brings new dividends to surrendering independence. Importantly, these benefits come in addition to the greater financial resources already available through donor money from states and agencies pushing those agendas.

If new technologies deliver on their promise of more efficient and effective humanitarian aid, then that financial bias may now be exacerbated by a technological one. This would presumably add to the political effectiveness of co-opting aid and to the material effectiveness of politicised aid, creating payoffs both for the co-opting government or non-government actor, for the humanitarian group in question, and for the populations that happen to be caught in areas controlled by those co-opting actors. Meanwhile people caught in other areas, accessible only to Dunantist groups on condition of an independence that requires them to forego several technologies, will not benefit. This would entrench a two-tier humanitarian system with evident political implications in terms of aid distribution.

[98] ibid.

## About the Authors

**Martin Stanley Searle** is an Associate Research Fellow at the Centre Non-Traditional Security (NTS) Studies, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU).

Martin worked 6 years with the international medical humanitarian organisation Médecins Sans Frontiéres/Doctors Without Borders (MSF). During that time, he worked in South Sudan, Central African Republic, Kenya, India, Bangladesh, Myanmar and Malaysia on a mixture of conflict response, healthcare exclusion, HIV and TB treatment, and migrant and asylum issues. He also worked at MSF headquarters on communications and advocacy for the South and Southeast Asia operational portfolio.

Martin holds a BA (Hons) in European Social and Political Studies from University College London, and an MA in International Affairs from The New School in New York City.

## About the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) is a think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education and networking, it produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

For more details, please visit www.rsis.edu.sg.  Follow us at www.facebook.com/RSIS.NTU or connect with us at www.linkedin.com/school/rsis-ntu.

## ***RSIS Working Paper Series***

*(from 2016 onwards)*

315 Is Use of Cyber-Based Technology in Humanitarian Operations Leading to the Reduction of Humanitarian Independence? (2018)
*Martin Stanley Searle*

314 Game of Institutional Balancing: China, the AIIB, and the Future of Global Governance (2018)
*Kai He and Huiyun Feng*

313 Xi Jinping and PLA Transformation through Reforms (2018)
*You Ji*

312 Comparing the Governance of Islam in Turkey and Indonesia: Diyanet and the Ministry of Religious Affairs (2018)
*Martin Van Bruinessen*

311 Indonesian Muslims in a Globalising World: Westernisation, Arabisation and Indigenising Responses (2018)
*Martin Van Bruinessen*

310 Theocracy vs Constitutionalism in Japan: Constitutional Amendment and the Return of Pre-war Shinto Nationalism (2018)
*Naoko Kumada*

309 Cyber Deterrence in Singapore: Frameworks and Recommendations (2018)
*Eugene EG Tan*

308 Trade Policy Options for ASEAN Countries and Their Regional Dialogue Partners: “Preference Ordering” Using CGE Analysis (2018)
*Xianbai Ji, Pradumna B. Rana, Wai-Mun Chia, and Chang Tai Li*

307 The South China Sea: Beijing’s Challenge to ASEAN and UNCLOS and the Necessity of a New Multi-tiered Approach (2017)
*Christopher Roberts*

306 China’s Belt and Road Initiative: The Evolution of Chinese Private Security Companies (2017)
*Alessandro Arduino*

305 Engaging Religion with Pragmatism: The Singapore State’s Management of Social Issues and Religious Tensions in the 1980s (2017)
*Mohammad Alami Musa*

304 Incident Prevention and Mitigation in the Asia Pacific Littorals: Framing, Expanding, and Adding to CUES (2017)
*Graham Ong-Webb, Collin Koh, Bernard Miranda*

---

Visit the RSIS website at www.rsis.edu.sg/?p=48639

to access the full list of past RSIS Working Papers.