Handle with care: Crowd-sourcing and non-proliferation

by Christian Dietrich

States do not spread weapons of mass destruction – people do. It takes individual proliferators, collaborators, and the acquiescence of bystanders for sensitive materials to change hands illicitly. Yet, the rigid national and international means deployed to counter proliferation are juxtaposed with the limitless amounts of information people produce in our digitally connected world.

The internet enables over one-third of the global population to gather in virtual, transnational spaces. 'Netizens' generate and process knowledge on anything from Wikipedia and cooking recipes to disaster management and counter-terrorism. In various fields, policy makers increasingly appreciate open-source information technology as an asset to feed their decision-making.

However, the use of information and communication technology (ICT) to counter the proliferation of weapons of mass destruction (WMD) remains an underdeveloped notion – particularly in light of its potential promises. Drawing on lessons from other policy areas, it is advisable to contemplate the systematic mining of collective intelligence for information gathering and analysis purposes in countering the spread of WMD.

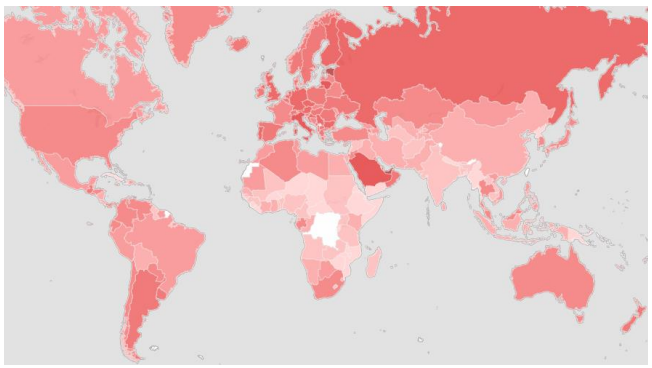
Hives of information

The digital divide splits the quality and scope of access to modern ICT roughly along global socio-economic lines. While mobile cellular subscriptions are rising at a remarkable pace in developing countries, the International Telecommunications Union estimates that less than one-third of the population in developing countries had internet access in 2013 – as opposed to over two-thirds in developed countries. Nonetheless, the existence of over 6 billion mobile phone subscriptions and 1 billion smartphones globally in the year 2012 is evidence of a significant trend.

The internet, with its various applications, empowers its users and democratises the process of collecting and interpreting information. Not only does it increase the speed of communication and dissemination; it also gives a voice to a greater number and diversity of authors. However, with new technologies usually come new problems, and ICT is no different. Data security and privacy are major issues of concern.

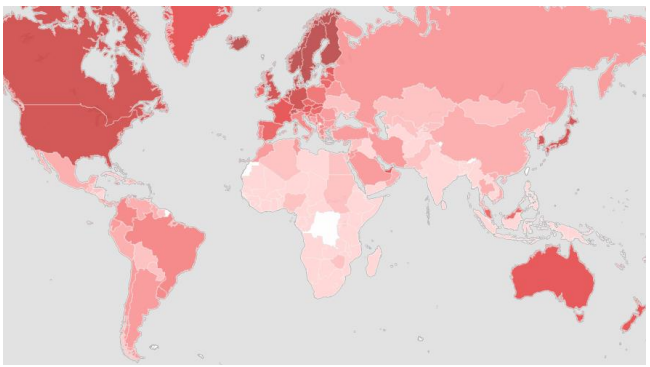
Methods of leveraging distributed networks of digitally connected individuals to gain information

Mobile cellular subscriptions (per 100 people)



Source: World Bank

Internet users (per 100 people)



Source: World Bank

are commonly subsumed under the term *crowd-sourcing*. It essentially comprises two operational modes: *knowledge-generation* and *data-processing*. In the case of the former – the bottom-up approach – web users feed information to an online platform. This allows the collation of information that would otherwise be inaccessible or would take longer to collect. In the case of the latter – the top-down approach – online volunteers analyse large data sets by completing a number of small tasks. The marginal contribution of each volunteer – processing a mere fraction of the overall data – thereby helps narrow down information that cannot be analysed by methods of automation.

With crowd-sourcing, levels of participation make all the difference. Given a sufficiently sized crowd, it can outperform many traditional organisations – be they media, private consulting, or intelligence. People can actively engage by generating or processing data in the same way as bees collect and process nectar. But they can also become the objects of big data analysis that helps understand the mind of the hive.

Tools of non-proliferation

As it stands, treaty-based verification to counter proliferation in the field of chemical, biological, radiological, and nuclear weapons (CBRN) entails checking a situation on the ground against states' treaty obligations – and making sure that declared items exist and that nothing sensitive remains undeclared. This is done by means of taking stock, inspecting, technical and conventional state surveillance, as well as sampling with respect to facilities, materials, and equipment. On top of that, export control arrangements aim to ensure that sensitive items do not cross political borders illicitly.

The concept and the practice of verifying the non-proliferation of CBRN weapons differ across the categories. With respect to nuclear weapons, the International Atomic Energy Agency (IAEA) keeps records of nuclear stocks, inspects and monitors facilities, and takes environmental samples.

Verification procedures against chemical weapons proliferation are more elaborate and established, not least because civilian and military (*dual-use*) applications of certain chemicals are much more intertwined. The Organisation for the Prohibition of Chemical Weapons (OPCW) oversees the destruction of countries' chemical stockpiles and monitors their facilities and industries. In contrast, the Biological and Toxin Weapons Convention lacks a formal verification mechanism.

Finally, radiological weapons – a combination of conventional explosives and radioactive waste from power plants or medical facilities – are the least addressed at a multilateral level. This remains the case despite growing fears about the diversion of radioactive materials to non-state actors.

Turning nectar into honey

The idea of crowd-sourcing in the realm of security is related to the concept of *citizen reporting* from the early 1990s. This envisioned an international regime under which states would grant their nationals immunity from prosecution were they to reveal information on their country's failure to abide by international treaties. It would also enshrine a citizen's right – and duty – to report acts of non-compliance to an international agency.

A January 2014 report by the US Defense Science Board suggests adding open online sources to the toolbox of nuclear monitoring and verification, with the help of cyber and big data programmes

akin to those of the US National Security Agency (NSA) – though preferably without the bad press. The forthcoming 2014 Nuclear Security Summit in The Hague, despite the fact that it has no record of meaningfully acknowledging societal contributions to nuclear security, could be a good opportunity to reconsider this use of ICT. In line with commonplace doctrines of deterrence, verification is more important the smaller the arsenals of WMD become. With fewer arms in existence, a higher value is attached to each weapon. ICT-supported citizen reporting could thus complement existing verification mechanisms in various ways, thereby also bolstering confidence in treaty compliance.

Regarding *data-processing*, remotely sensed information – such as satellite imagery – could be fed to an online public for preliminary analysis. For instance, in response to Typhoon Haiyan that struck the Philippines in November 2013, online volunteers analysed satellite images and created annotated maps of the devastated areas that were subsequently used by the United Nations and other relief agencies.

In a similar vein, volunteers could sift through data to look for suspicious construction projects or movements. Overhead commercial, declassified, and historical imagery of large areas could be 'mined' in search of explosion test sites. Algorithmic filters and statistical and expert analysis could help consolidate the findings and ensure quality control, making the resulting data more reliable and manageable. This could also be a valuable addition to the monitoring activities of the OPCW and the Comprehensive Nuclear-Test-Ban Treaty Organization.

Knowledge-generation based on citizen reporting could have multiple uses in countering the spread of WMD. The Kenyan presidential elections of 2007 may serve as an example of the digital collation of data based on eyewitness accounts. Volunteers reported acts of political violence via text messages, email and Twitter that were then consolidated into an interactive online map by the non-profit software developer Ushahidi.

Platforms could be provided for people to report suspicious occurrences. Images and information by witnesses of illicit transfers of knowledge or materials could be communicated anonymously to platforms hosted by the lead agencies of the respective WMD regimes. Moreover, maps of suspicious, alleged, or confirmed incidents of trafficking of sensitive materials could be based on data from various agencies and experts around the globe to help detect trends and track movements. This would, *inter alia*, increase the chances of identifying diversions of WMD to terrorist organisations.

Lastly, *big data* – the 'digital exhaust' that netizens leave behind – can be used for near real-time monitoring. For instance, the 2010 cholera outbreak in Haiti could have been detected up to two weeks earlier if the numerous signals on social media had been picked up in a systematic manner.

Big data analytics could help pick up information relevant for countering WMD terrorism, and could also serve as a tool to detect and collate witness accounts – although such communication often merely addresses the online ether rather than specific authorities. For example, researchers have used social media analytics successfully to detect ceasefire violations in Syria within minutes.

There are, of course, particularities in verifying non-proliferation of different kinds of WMD. Nevertheless, crowd-sourcing can become a key piece of the puzzle in informing and streamlining political decisions in times of urgency; and it would grant greater ownership to national and global civil society.

The inevitable sting

Getting non-traditional actors involved in WMD non-proliferation poses certain technical and conceptual challenges. Between being overlooked and becoming a loose cannon, a delicate balance must be struck by authorities to make participation a mutually beneficial experience, while pooling and sharing control over the process.

In order to preclude unintended consequences, cumulative errors, and malicious manipulation, those who seek volunteer-generated information must clearly communicate the parameters of any such project, thus facilitating an open process while steering it in a content-neutral fashion. Data analysis should, ultimately, be the prerogative of algorithms and professionals – for all their flaws – before any judgement is passed by authorities or experts.

Another cluster of issues revolves around access to data – and to the hive as such. Governments tend to have a monopoly on substantial sources of intelligence as these are deemed vital to national security. Furthermore, certain aspects of WMD are simply considered too sensitive for the public because they might pose proliferation risks in themselves.

Threats to the openness of the internet (not exclusively, but especially in authoritarian states) exacerbate the issue and may impede international ICT-based solutions. Recent revelations about the activities of the NSA also suggest that any crowd-sourcing be based solely on open sources and held to high accountability standards. Regionalised applications could help ease into larger citizen involvement in the endeavours as ICT-users invariably become more tech-savvy. Developers must also provide citizen reporting with an infrastructure that offers, at a minimum, a secure and password-protected environment (encrypting communication and thereby rendering it anonymous) to safeguard sensitive sources.

What is more, few people are aware of the legal frameworks regarding WMD. While the Syrian civil war regrettably prompted chemical weapons to rise to prominence once again, WMD will struggle to maintain sufficient salience for sustained crowd-sourcing. Meanwhile, the quality of crowd-sourced data crucially depends on the public interest in the endeavour. Making *data-processing* a playful and visually appealing experience has proven to be a good starting point to ensure and sustain this interest.

Crowd-sourcing could also exacerbate the political cleavages between developed and developing states along the digital divide. Projects should therefore aim to target and balance the distribution of their participants as much as possible. And its products should be treated as collective and open resources.

Whether crowd-sourcing would pose more of a security risk than add value will have to be determined on a case-by-case basis. While having the potential to surpass traditional methods of intelligence gathering, it faces an uphill battle against the secrecy that surrounds WMD issues.

Although challenges abound, none of them are intrinsically insurmountable and any project that acknowledges them is off to a good start. Additional research and incremental implementation in various policy fields can significantly drive forward the learning process of how to best employ crowd-sourcing.

The EU as beekeeper?

Both the 2003 European Security Strategy and Strategy against the Proliferation of Weapons of Mass Destruction acknowledge that countering the threat of WMD proliferation is key to international security. However, no major EU document mentions a possible active role of citizens in countering proliferation. While much of the constituent parts to operationalise crowd-sourcing projects in an EU framework already exist, the dots have not yet been connected.

The EU has ample research expertise to develop its own crowd-sourcing methodology, and conducts cutting-edge research on actual and potential uses of ICT in crisis response and civil protection as well as related ethical issues through the Commission's Joint Research Centres. It also funds a variety of projects and institutions that embody the non-proliferation infrastructure and the expertise needed to guide crowd-sourcing projects. Its CBRN Centres of Excellence initiative represents a decentralised effort to provide consultancy services – and a hub for cooperation. In order to build a platform for dialogue between research centres and policy makers, the EU also created a consortium of European non-proliferation think tanks.

The Union is also equipped with intelligence bodies that could contribute to (and profit from) crowd-sourcing platforms. The EU Intelligence Analysis Centre, which coordinates intelligence operations according to threat assessments, could be at the heart of these efforts by hosting a platform for non-proliferation crowd-sourcing that is fed with data from several EU bodies, such as the EU Satellite Centre.

While airtight detection and prevention of WMD-proliferation using current means is impossible, crowd-sourcing is no panacea either. At this stage, sponsoring the active use of open-source information technology and crowd-sourcing to promote non-proliferation would allow the EU to adopt a pioneering role as a beekeeper. It could work out quite well, but there will be stings along the way.

Like most beekeepers, the donning of protective gear is in order, with smart infrastructure and responsive facilitation providing just that. But this alone will not do. In order to harvest the hive's mind, it needs to be given a home and engaged with. Between over- and under-regulation, and between too much and too little privacy, crowd-sourcing can help counter the threat of WMD falling into the wrong hands. The EU has a chance to be at the cutting-edge of this emerging practice. Meanwhile, potential proliferators will not stand idle.

Christian Dietrich is an Executive Research Assistant at the EUISS.