THE DIGITAL SECURITY OF THE JOURNALISTS IN DISTRESS NETWORK

EXECUTIVE SUMMARY

This report assesses the digital practices and vulnerabilities of a global network of human rights organizations that operate similar emergency assistance programs. These programs provide humanitarian assistance to journalists and other media workers around the world who are persecuted because of their work. The global Journalists in Distress (JID) network faces the challenge of adapting to the rapidly changing digital contexts in which its member organizations work.

The member organizations of the global JID network collectively disperse a majority proportion of the total global funding for emergency assistance that is available to journalists in distress. In other words, this network represents the vast majority of the organizations (which are not part of a United Nations or European Union governing body) that do this type of emergency assistance work around the world. Financial support is typically provided to cover legal fees when journalists are detained, medical expenses when they are caught in the line of fire or traumatized by their coverage, transportation costs when they are forced to flee, and short-term resettlement costs (including living expenses such as lodging, food, and Internet access) after escaping a dangerous country or situation because of their work.

The global Journalists in Distress (JID) network was formed in 2006 to allow organizations with international free expression mandates to more easily discuss specific cases, coordinate joint efforts, avoid duplication, and direct at-risk individuals to resources that can provide them support. Comprised of between 15 and 20 organizations at any given time that have different sized budgets and other resources, throughout its years of operation the JID network has disbursed millions of dollars to journalists and other media workers in danger around the world.

In 2015 alone, the network dispersed over $4 million USD to more than 1500 people (journalists, writers, and human rights defenders). Any digital security vulnerabilities within this single network can have serious, real-life consequences for a population of thousands of at-risk, persecuted individuals and their families. To help address these risks, data about the current digital practices being employed by the network's member organizations was collected in fall 2016 and is presented in Part 1 of this report. In Part 2, these digital practices are evaluated for the digital security strengths and vulnerabilities they afford the network as a whole. The discussions in both parts of the report are organized into three sections concerning the digital security of the JID network: 1) Cyber devices, 2) Communications, and 3) Digital security within member organizations.

Part 1 begins by describing the devices used by member organizations to access JID data and their levels of encryption, password protection, and security updates. The network members' thoughts on the security of their main modes of communication are described, as well as their frequency of communicating with one another and their decisions to *not* share sensitive data over the Internet due to security concerns. The methods used to discuss emergency assistance work with colleagues within their organizations, with non-network contacts, and with applicants to their programs are discussed. This part

also presents the findings about the transmission of JID data to and from different geographical regions and countries, and it is accompanied by the locations of the network member organizations and the frequency with which their staff travel to elevated risk locations. The frequency with which network members think about digital security and worry about their Internet communications being monitored are also described, as well as their levels and sources of digital security training, and sources of help for technological problems they encounter during the course of their work.

Part 2 discusses the physical vulnerabilities that exist to the JID network members' cyber devices, despite most of their staff working in low risk locations. The members' compliance with the network's ground rules concerning digital security are presented, as well as the trends that emerge from these findings. The practices that members use to remember, store, and change passwords are also discussed. The strengths and weaknesses present in the many types and modes of communication within the network are described, including the various software that variously increase or decrease the security of the network's data. The state of the Internet and press freedom in the most common countries to which JID data is sent and received is mapped, showing that the majority of these countries are deemed 'not free'. In the final section, the ways in which JID network members evaluate and sustain their organizations' own digital security are discussed, given that if members are not taking their own digital security seriously, the network's digital security will suffer in turn. An important part of these practices are the staff's work routines, including the amount of time they can spend on emergency assistance work, their individual workplaces (at an office or home), and their teamwork or autonomy.

AUTHOR

Taryn Blanchard is the Programs Coordinator at Canadian Journalists for Free Expression (CJFE), a Toronto-based non-profit organization that works to promote and protect freedom of expression and access to information in Canada and around the world. She is also a PhD candidate in the Department of Anthropology at the University of Toronto, where she researches free expression advocacy in today's digitally mediated world, with a focus on how transnational human rights networks are built and used strategically by activists and individuals at risk.

To contact Taryn, please email tblanchard@cjfe.org or taryn.blanchard@utoronto.ca.

OPEN TECHNOLOGY FUND

CJFE