APPG ON CYBER SECURITY MEETING MINUTES 4th July 2022

Title: Cyber Security and Humanitarian Aid

Chairman's welcome – The Chairman welcomed everyone to the meeting and introduced Dr Williams.
Present: Simon Fell MP, (Chair), Lord Arbuthnot of Edrom
Apologies: Admiral Lord West, Baroness Neville Jones, Baroness Neville Rolfe, Lord Mackenzie of Framwellgate, Lord Taylor of Warwick, Sir George Howarth MP
Speaker:

1) Dr Olivia Williams

Dr. Olivia Williams works in a national security capacity as a senior Cyber and Information Security consultant with the Defence company Apache IX (pronounced Apache 'eye-ex'). Prior to this, she worked in the Aid sector where she deployed to natural disaster and conflict environments across Malawi, Nepal, the Philippines and Northern Iraq. She is a Ph.D graduate of American University in Washington D.C. and currently working with International Politics department at the University of Aberystwyth to develop an aid organization-focused cyber-attack database and data analytics hub named AidInfoSec. Olivia will be sharing her doctoral research and findings with us on the topic of her Ph.D thesis namely, information and cyber security risks on the humanitarian frontline, and discussing how vulnerabilities specific to that context can result in real world harms against some of the world's most vulnerable communities.

Dr Williams has worked in the Aid sector since 2013. She has observed how communications technology for data collection/processing and sharing and handling has increasingly become the norm. Handing over personal data by a refugee is often the key to receiving aid. The data gathered can vary but typically covers: Names, DOB, medical and shelter needs amongst other personal data and can also include religion, ethnicity or political alignments – many of which are legitimately needed. These create a 'digital dossier' on individuals and these proliferate widely as this data helps with the delivery of aid and the definition of individual needs / requirements. Aid agencies may also gather climate and other geopolitical data on a project.

Dr Williams found that personal data can be used to further the priorities of threat actors as well as legitimate ones. Humanitarian data can become a "weapon" and Dr Williams realised that in the field no-one was looking at/discussing data protection. This led to a series of research questions and Dr Williams described her research methods of content analysis, electronic survey and interviews.

Dr Williams discussed a number of cyber attacks which have happened. This includes the bugging of electronic communications. Aid agencies do not typically share information about attacks with any central repository and information for aid workers on cyber hygiene or what to do if attacked is sparse. Typically aid workers are de-briefed on their return home about various

concerns/experiences related to a deployment. However, none of the aid workers electronically surveyed as part of Dr Williams' research had ever been asked about their data handling experiences or asked for feedback relating to their in-field data-handling.

An NGOs beneficiaries are generally not informed about the purposes of data collecting or handling nor are they informed of their rights over their data (right to deletion, right to obtain a copy of their information etc). Although many of the NGOs interviewed indicated that their in-country offices are GDPR compliant – even those outside of the EU, Dr Williams doubts that this can be the case.

Dr Williams shared a number of research findings at the meeting:

Data Handling:

- Significant number of aid workers use their own devices to collect, process and share beneficiary data, and have not been instructed by their NGO not to do so.
- Devices and papers containing beneficiary personal data kept in locations where unauthorized persons could access them.
- Devices were often protected by a password or PIN as well as hidden in physical locations. Although AV equipment was also hidden, they were not digitally protected.
- Email most common means of sharing beneficiary data, but physical handover of beneficiary file or USB stick and use of messaging apps and phone calls to share data also relatively common
- Only some aid workers confident in limiting access to data stored or uploaded to an online repository or third-party platform
- Aid workers 'trusted' that onward safeguarding would occur, rather than checking by any other means.

Cyber Attacks and Attack Surfaces:

- Only some respondents were able to explain Malware and password attacks
- majority responded that they had never heard of whaling, pharming, man-in-the-middle or cyber drive-by attacks.
- only a few replying that they could explain a spear-phishing (37.9%) and eavesdropping attacks (43%).
- 'cyber attackers purposefully attack NGOs', the majority (53.1%) responded said that they 'weren't sure' with others replying, 'no they're not specifically targeted'.
- hotel WiFi was the most common internet connection point used to share beneficiary data with colleagues and other organizations.

Aid Worker Awareness:

- Common types of cyber attack are little understood by aid workers
- Majority of aid workers understand the need to protect data throughout the data lifecycle, but some suggested that protections were only 'sometimes' required, whilst a few others said they was 'never' necessary.
- Protecting data during collection and dissemination important, during processing not so much.
- Data protection training of aid workers is irregular, with high number of those who had received it saying it was 'inadequate' and not fit for purpose.
- Many aid workers never received a debrief. The majority of those who had received one within the past 5 years expressed that they'd never been asked about their data handling experiences
- Applying NGO policies to field settings is unrealistic

Aid Worker Publicizing of Personal Data:

- Personal and sensitive beneficiary data publicized across online and offline spaces. Predominantly via social media but also postings on websites and in e-newsletters
- Some aid workers had shared a beneficiary's real name, physical address, location or GPS coordinates, email address and telephone number
- Aid workers who had shared beneficiary data had almost all had shared a photograph of a beneficiary's face, and a smaller number had posted video and audio recordings of beneficiaries too.
- Beneficiaries rarely informed of their rights

Open questions and discussion –
SF – given that you have outlined the difficulties around cyber security in this sector, how do we take your findings forward?

OW – an independent organisation that collects and shares data would be a good start. This does not exist now but the enterprise I'm founding called AidInfoSec which will be held at the International Politics Department at Aberystwyth University, is an attempt to plug this gap. It is similar to the terror attack database[1] run by the University of Maryland. Secondly, helping organisations adopt NCSC practices and thirdly, experts to offer pro bono know-how to Aid Agencies. This all needs to be raised in Parliament or NGOs will be left out of the cyber security equation.

[1] Global Terrorism Database (umd.edu)

Lord Arbuthnot – In the Falklands internet coverage is poor due to geographical reasons. Satellite communications are expensive and unreliable there. How do you get round these factors and human nature which will go for the most convenient outcome?

OW – it is about managing people and their behaviour, providing education, training as well as plenty of real life examples – these are key.

Arnoldis Nyamande – gathered that a lack of professional standards is a root cause of the problem. The Chartered Institute for IT promotes ethics. Do you think that HQ-based or field-based aid workers should learn data protection etc.?

OW – agrees. The ICRC[2] attack is well known from earlier this year. They are good at putting policies in place but these do not filter down. Training needs to be broader and better funded. Perhaps the World Bank or the FCDO have a role to play here in insisting upon a certain standard of data security as well as adopting a spot check practice?

Professor Keith Mayes – what is best practice for NGOs and who would define this?

OW – not clear which set of practices apply to NGOs. Their work is so varied and it can be hard to apply in context. Cartong[3] have excellent documentation which provide set examples inspired from real world contexts which provide a storytelling approach to this entire topic. These help aid workers to quickly apply stories to their own lived experiences/contexts. .

Professor Mayes – can I suggest that you create a strawman proposal?

Andrew Fleming – I have investigated a number of NGOs in the past and prosecuted their staff for financial crime. We are all aware that information has value, so how to you manage training, data sharing, controls etc. and make staff understand that there are consequences for their clients if it is mismanaged?

OW – Balance between managing people closely and giving them a large degree of autonomy. Behaviours have to be managed. I am trying to build a process to guide behaviour.

Malcolm Warr – was at CHOGM 2002 when what we are discussing today was talked about. Also covered at Davos and CHOGM 2022. The communities which you are trying to help needs to be protected. Promoted digital society in Rwanda. There are global baseline schemes, should UK plc be promoting them?

---

[2] Cyber-attack targets data of International Committee of the Red Cross
[3] About us | CartONG

OW – there is resistance from beneficiaries to their data being collected in some places. Some do fear that their own data will be used against them. The downside of not providing personal data is that these individuals do not receive aid. Data security and privacy fall down the priority list when faced with the alternative of no shelter, no food/water, no protection.

AF – How can we ask a refugee to give away all their personal data especially biometrics without being about to guarantee the safety of that data. Should data gathering not be Proportionate, Legitimate (Legal) Accountable and Necessary (PLAN)? This aligns to GDPR as well as other data protection requirements. There should be no fishing expeditions for data just because we have the power to request it?

OW – you do need certain items of data to process the refugee. Generally, aid workers do not apply basic data security principles such as data minimization. Clearly you do not need to take exact names for some actions and could pseudonymise personal data. Tendency is to collect too much data. There needs to be a cross-organisational and cross-territory standard for this outside of the West where regulations such as HIPPA or GDPR have no authority.

Ben Stanley – seem to be three factors at play here: lack of resources, knowledge and awareness. Buy-in is key. Is there anything you can point to?

OW – UN is pushing for more local aid workers to be hired. Cyber security and a real assessment technical ability has not been a factor in hiring local people. Professional aid workers can be trained of course, but as soon as you hire local people with a lesser level of IT literacy you are open up to problems. It is the big “elephant in the room”.

Andre Turville – Do you see any insider threats through local recruitment?

OW –My study wasn’t looking at this problem through the lens of local recruitment so I can’t say, however, I would be surprised if local recruitment in some contexts and locations didn’t greatly affect the security of beneficiary and organizational data.
MW – Could cyber essentials be an exportable item?

Simon Fell - the real challenge is in balancing cyber security with saving lives, carrot vs stick. What is your view on funders requiring a standard of cyber security? Would that drive behaviour?

OW – yes it would force a change in behaviour. However with such a high turnover of staff it would be hard to operate and to ensure that the change filters down. It would go some way towards helping though.

AF – information has power! If it is correctly used that is great, however, if wrongly used then that can be very bad, and it can have fatal consequences in some cases. There must be consequences for NGOs to ensure that they do the right thing. One should also put training in place first before putting staff into the field, start with the best intention. Why not use biometrics to protect access to devices and sensitive data?

OW – yes, there need to be a greater discussion on this. Dutch and Scandinavian NGOs are much more transparent and candid as they have a premise of transparency baked into their cultures. We are taking baby steps towards a culture of transparency, but there is a danger of pushing problems underground and out of view if we go too fast. Biometrics for anyone beneficiary or aid worker is problematic as the data collected via that means is sotred somewhere and potentially recoverable and exploitable not only by aid organisations but also by threat actors. I do not use facial recognition for my Defence laptop for example even though it possesses that function. The issue is around personal privacy and security and how we balance privacy vs surveillance. Currently privacy literature and security literature are in separate siloes where one it is believed must supersede the other -what we need to try to achieve is a reality where both can be balanced equally across the Information Age and personal data landscapes.

Frederic Gibaudan – why not substitute a name for a pseudo-ID. The Aid sectors needs better understanding about what can be done.

Conclusions – Simon Fell thanked Liv Williams for speaking and in particular for being the only one today. He also asked the meeting to let him know if anything should be raised in Parliament.

Next meeting – TBC