Utilization Focused Evaluation Final Report

Summary for Workshop Feedback, KEQ1, KEQ3, and UFE Lessons Learned

Written by Jennie Phillips, Evaluator

November 2014

Table of Contents

Executive Summary

The following report summarizes Citizen Lab's experience with implementing Utilization Focused Evaluation (UFE) with the Cyber Stewards Network (CSN) project. This project was a collaborative effort between the Citizen Lab, International Development Research Centre (IDRC) and the DECI-2 research group and mentors. It was implemented for the full duration of Phase 1 of the CSN project.

This project is discussed in sections:

Introduction – introduces the project, provides background, explains data collection approaches used since the last UFE report, and describes the scope of the report.

Part 1. Analyzing Workshop Feedback – Summarizes participant survey responses from the second CSN workshop

Part 2. KEQ1 Analysis – Summarizes outcomes from Key Evaluation Question 1, specifically analyzing year 1 and 2, and providing recommendations for the next stage of the project on this question

Part 3. KEQ3 Analysis – Summarizes data collected on security and resilience (data for KEQ3) from the most recent workshop, and provides recommendations for this question in the next stage of the project.

Part 4. UFE Lessons Learned – Summarizes the UFE process used by the Citizen Lab, successes, challenges, impacts, and provides recommendations for future applications of UFE.

Conclusion – Summarizes the impact of UFE and project usefulness

Utilization Focused Evaluation | Final Report
Summary for Workshop Feedback, KEQ1, KEQ3, and UFE Lessons Learned

Introduction

The Cyber Stewards Network (CSN) is an initiative led by The Citizen Lab in partnership with the International Development Research Centre (IDRC). The aim of the project is to build the capacity of civil society groups in the global south working to promote human rights freedoms online. The Lab has employed Utilization Focused Evaluation (U-FE) to help identify the needs of the partners and facilitate the development of their capacity and a larger network. To date the Citizen Lab has hosted three workshops with the CSN, two, of which, have involved UFE.

A. Project Background

There are three aspects of this project that the U-FE process seeks to support:

1. Network Development
2. Research & advocacy
3. Resilience & Security

The three Key Evaluation Questions (KEQS) identified include:

1. How can network partners support one another to maximize influence and impact at their local, regional, and/or international level?
    - What is the role of the citizen lab, as a network facilitator?
    - What is the role of the cyber stewards, as network partners?

2. How can communication be improved between network partners for the sharing of skills, knowledge, tools, etc.?
    - What is the role of the citizen lab, as a network facilitator?
    - What is the role of the cyber stewards, as network partners?

3. How can security and resilience be assessed and developed in a networked project?
    - What is the role of the citizen lab, as a network facilitator?
    - What is the role of the cyber stewards, as network partners?

B. **CSN Workshop 3**

Description

The third CSN workshop was held in Toronto, ON after the Cyber Dialogue from April 1 to 3, 2014. With a total of 24 participants in attendance, the workshop included cyber stewards, partners from Privacy International network, IDRC representatives, MacArthur foundation representation, Citizen Lab staff and partners.

The primary objectives of this workshop were to gauge partner progress on projects, facilitate collaboration, enhance research communications, progress collaborative research projects, and continue capacity building on risk and security. The design of this workshop was informed by U-FE, more specifically KEQ2 and KEQ3, and survey data collected from the previous workshop (see Part 1.Analyzing Partner Feedback) as well as administrative needs. The majority of the workshop was designed to address the ResComms piece of the DECI project, however there were some elements of UFE that were included. The workshop was structured as follows (see Annex A for a full agenda):

Day 1	Project updates
Day 2	Research communications special presentation by Ricardo Ramirez from the DECI-2, Research communications and the CSN, and breakout sessions for collaborative research projects
Day 3	Security exercise, breakout sessions continued

Each of these activities is described below.

Activities

The following is a description of the activities completed with CSN members.

1. **Project updates** - all CSN partners were asked to present for approximately 10 minutes on the following 3 questions:

    1. What have we achieved so far?
    2. What challenges have we encountered?
    3. What can we do to help each other?

    All presentations gathered and shared on the CSN Google drive. Ask CitLab staff for access if required.

2. **Research communications special presentation -** Ricardo Ramirez, one of the DECI-2 partners, provided a brief seminar on developing a communications

strategy for policy influence.

3. **Research communications and the CSN** -- Select CSN partners provided presentation on elements of research communications:

    1. Shahzad and Ramiro: *Research / Advocacy and Public Litigation*
    2. Donny and Gbenga: *Research / Advocacy and Public Policy*
    3. Olga and Lobsang: *Research / Advocacy and Community Outreach*

4. **Breakouts for collaborative research projects** -- time was allocated for partners to continue work on the collaborative projects identified in the CSN workshop 2 (Indonesia) listed below:

    1. *Project 1: Mapping the Infrastructure, Policy, and Practice of information control in the Global South*
    2. *Project 2: Multidisciplinary Analysis of Political Events and Information Controls*
    3. *Project 3: Impact of Information Controls on Digital Rights Activism*
    4. *Project 4: Information Control Research in High Risk Areas*

    In addition, time was also allocated to respond to other participant driven needs identified. A seminar on targeted threats / malware was also offered in one afternoon for participants.

Security exercise - a mini-table top exercise was run with the CSN using a sample case experienced by one of the CSN partners to explore how the situation was responded to, to solicit suggestions for future response, and identify network interest and capacity to support one another in a crisis. The presentation used to guide discussion is provided in Annex J. This was the first in hopefully a series of simulations.

C.Data Collection

Prior to, during and post CSN workshop 3, there were a series of data collection events to gather data for the UFE questions. Activities are outlined below.

Surveys

Three surveys were distributed prior to the workshop.

1. **Survey 1. Planning Survey for Workshop 2 (Annex B)** — Used to identify areas to cover in the upcoming workshop, and lessons learned from the previous workshop. Responses were used to design the agenda for the 3rd workshop. Twelve responses were received.

1. **Survey 2. Security Protocol Development (Annex D)** — Drawing from risks identified in the 2nd workshop, participants were asked to select their three highest risks and describe the situations of low, medium and high impact. The aim of this survey was to contribute to the identification of crisis activation levels. These levels are to be used to describe the different response strategies that must be activated by the lab and network during a crisis. Responses from this survey were used in the draft development of the Security Protocol Document, and design the crisis simulation for the 3rd workshop. Four responses were received.

1. **Survey 3. Resilience Assessment (Annex E)** — This survey asked participants to complete the Resilience Assessment Survey for NGOs developed by ResOrgs[1], New Zealand, and to reflect on the suitability of the survey for their context. Responses from this survey were used to guide resilience interviews, and also, influence the design of the crisis simulation during the workshop. Six responses were received.

Interviews & Focus Groups

Outside of workshop time, the evaluator met with the participants who engaged most in survey 2 and 3 to discuss the notion of resilience, the resilience survey developed by ResOrgs (2013), and brainstorm a resilience CSN network. Six participants were interviewed in total. See Annex G for the questionnaire used.

Security Exercise

Note-taking was used to record participant conversation during the simulation.

[1] Abraham, B., Seville, E., Hatton, T., & Vargo, J. (2013). *A short guide to resilience for NGOs* (pp. 1–11). Resilient Organizations. Retrieved from http://www.resorgs.org.nz/images/stories/pdfs/resilience-within.pdf

D.Scope of Report

This report aims to serve four purposes:

1. **Workshop Feedback** - Analyze and report on participant feedback from the second and third CSN workshop in Toronto, ON
2. **KEQ1 Analysis** - Report on lessons learned, assumptions and challenges for Year 1
3. **KEQ3 Analysis** - Summarize and synthesize data collected from the third workshop in Toronto, ON to answer the third UFE key evaluation question (security and resilience)
4. **UFE Lessons Learned -** Reflections on the application of UFE throughout the duration of the first year of the project.

Note: Analysis of data collected for KEQ2 is not included, as it is considered under the research communications element of this project, and is thus not part of the UFE reporting process.

PART 1. Analyzing Workshop Feedback

A. Objective

This section of the report will summarize participant feedback received about the workshop in Indonesia and requests for the sub-sequent workshop in Toronto.

B. Participant Feedback

For a full summary of data collected refer to Annex C.

Evaluation of CSN Workshop 2 (Bali, Indonesia)
Participants enjoyed the interactive and participant driven design of the workshop, the opportunities for knowledge sharing, and embedded instances of reflection (morning debriefs). They felt, however, that more time should have been allotted for activities and working groups, as well as for CSN members to discuss their individual needs specific to their projects.

Planning for CSN Workshop 3 (Toronto, ON)
Participants requested secure network communication, knowledge sharing and network development as the primary themes to be addressed in this workshop. They wanted to more time as a network and in working groups to share lessons learned, solicit feedback on their projects, and pursue collaborative research ideas.

CSN Development
Participants felt that the CSN helps support their work on the ground through expanding contacts and opportunities for collaboration, knowledge sharing on regional issues and alternative advocacy strategies, and through the provision of research to support their advocacy activities. To enhance support, they felt they needed additional mentorship and enhanced collaboration, increased visibility with the network and access to high quality research, and more secure ways of communication.

PART 2. KEQ1 Analysis

A. Objective

The following sub-report is a reflection on the lessons learned, assumptions and challenges associated with reflecting and looking forward on the Cyber Stewards Network (CSN) project run by the Citizen Lab (CL). This discussion will focus on the first Key Evaluation Question (KEQ) associated with the Utilization Focused Evaluation (UFE) component of the project. The KEQ1 is as follows:

- *How can network partners support one another to maximize influence and impact at their local, regional, and/or international level?*
    - *What is the role of the citizen lab, as a network facilitator?*
    - *What is the role of the cyber stewards, as network partners?*

This question will be assessed by analyzing the following themes: network building, support / capacity building, influence and impact, and roles.

B. Network Building

Year 1 | Lessons, Assumptions

Network definition

One of the formalized aims of this project is to create a network. In the first DECI meeting, CL partners identified that at that the CSN at that time was not a network. Hence the first KEQ emerged, as a means to work towards developing a network. At present the CSN project remains a formal network. It is fairly clear at this point that if the CL or IDRC were to retract funds and/or pull out of the project the network would collapse. That being said an informal network has started to emerge. It is unclear what the future for this portion of the network looks like, but we will pay close attention to how it develops

Unified Vision

Mission Statement - Preliminary discussions with the DECI group sparked that idea that generating a common vision might contribute to the development of a network. In collaboration with the stewards, a mission statement was drafted and created. This activity drew little interest from partners, however, and at present the mission statement is more of an administrative component the a cohesive vision for the CSN. It seems as though the development of a mission statement had minimal to no impact on the development of the network. In addition, partners expressed their distaste for the global north / global south divide in the CSN workshop 3.

Collaboration within CSN

Over the past year we have observed that partners are collaborating on an increasing basis. We can use the following indicators to make this claim:

In between meetings (Remote operations)

- Frequency of contact with the cyberstewards.org mailing list - the mailing list is being used more frequently, and by a wider variety of users than at the start of the project
- Nature of mailing list conversation - In addition to sharing project updates, the cyber stewards are starting to engage with the mailing list when they need support e.g. Petitions, feedback on reports, campaigns, to suggest potential avenues / contacts for collaboration
- Collaboration - although mild, some partners have worked together e.g. CIPESA and PIN
- When partners go to conferences they contact one another and connect in country

During meetings (centralized)

- Nature of conversation - partners demonstrate sincere interest in hearing about what other partners are working on and working together to help them overcome barriers
- Trust - partners are willing to engage in more sensitive / vulnerable conversations
- Collegiality - partners are more friendly with one another, engaging socially after hours with one another
- Pride - partners express appreciation to be a part of the network, and value to their involvement
- Co-generation of ideas - in workshop 2 & 3, partners were keen to co-construct research project ideas

Although partners are starting to collaborate, the CL sees the potential for further, more in-depth collaboration. The assumption is that partners need to work together more to facilitate knowledge sharing and foster network development.

During the CSN workshop 2, partners identified 4 research topics together that they were interested in working on. These areas included:

1. Comparative Case Studies on State Responses to Incidents
2. Surveillance and Legal Contexts – Building a Standard Framework
3. Psychosocial Impacts of Digital Activism
4. Research in High Risk Areas

The ideas gained traction during the workshop, as partners were keen to meet prior to breakfast daily to discuss how to progress the potential papers. One of the groups met once via Skype in early 2014, with intent to meet again but the meeting date is yet to be determined. The assumptions for why these research projects lost momentum include:

- Funds discussed but not committed to projects
- Leadership was unclear — it was unclear if and who wanted and could lead the projects
- Capacity building in research methods required
- Competing priorities made it difficult to prioritize a new project over their own

During CSN workshop 3, partners were paired up to present work during the research communications component of the workshop. Themes included research advocacy & public policy, public litigation and Advocacy & Community Outreach. The nature of the presentations combined with the discussion made it evident that there is room for more knowledge transfer in the network at that partners would benefit from working together more. It's assumed, given engagement in the discussions that partners are interested in working together. It is unclear, however, who would like to work together and how well they will work together.

Later in the workshop, one of the partners requested a tool that could track the different skills, aptitudes, tools, initiatives, etc., for each partner so the network has more detail about the capacity of each member. This was suggested as a means to facilitate collaboration. Based on this suggestion, the assumption is that partners are unclear about the specific capacities offered by each network member.

In addition, partners have requested for a virtual space to access and share tools with one another more. The assumption is that they will use the space, and that creating a virtual space for file sharing and discussion will contribute to collaboration.

Collaboration with other Networks

CSN & CL Network Integration - Following first DECI meeting, the idea was proposed to create a larger CL network and use the CSN as “stewards” for the larger CL network. The meeting ended with the idea lingering in the minds of the PIUs. Over the term of year 1 of project, the focus shifted back towards developing just the CSN given the challenges with developing the small network alone. The decision was to focus small on the CSN, and then expand to the larger CL network once the CSN is more stable

CSN & Privacy International (PI) Network Integration - Given overlaps between projects, partners, and IDRC as a common funder, efforts were made over the year to collaborate with PI and bridge our two networks. However, we have encountered challenges in coordinating with PI program officers and as an alternative have focused on trying to connect partners ourselves. PI program officers and network members members have attended our workshops, and we have attended theirs. There appears to be interest between the networks to collaborate, but it has been difficult to coordinate the streamlining of both networks. As such, the CL has decided to integrate networks at the grassroots level and invite PI partners directly to our workshops and into our network instead of going through the PI hub. We hope to have a meeting with PI program officers before phase 2 of the CSN project begins to discuss potentials for collaborations going forward.

Social Network / Trust building

Social Activities - In a recent discussion with one of the CSN partners about comparison between networks which they are a part of, they claimed that the CSN felt more like a network than some of the others. They identified the exact moment when the group started to feel like a cohesive network - Indonesia. It was during this time that partners were together for 2 weeks, 1 week at our workshop and 1 week at the IGF. During this time, beyond workshop hours… they had a lot of time to be social and get to know one another. In discussions with other partners, many of them trace the transition for being network partners to colleagues during this time… and more specifically during the day trip to a temple in Indonesia. This experience has shown the importance of including social aspects during workshops to build connection, trust, and support between one another.

Security Exercise - During the workshop 3 partners had the opportunity to run through the simulated recent crisis faced by Bytes for All. A topic that was incredibly vulnerable for Shahzad to discuss, partners expressed sincere interest in understanding his situation, asking questions, and providing advice. When asked if partners were interested in supporting one another during crises, the entire room put up their hands. Running through this exercise allowed partners to engage on a deeper level with one another, and start to articulate a bond that can support one another.

Year 2 | Moving Forward

To accommodate the lessons learned from the previous phase the following actions will be taken

- **Collaborative Projects** - Formalize the collaborative research process, and request partners propose and engage in collaborative projects for the next round of the project instead of individual projects. The assumption is that if we provide funds for the research, and research support, partners will be able to prioritize and contribute on a collaborative research project.

  Building on the research project ideas generated in workshop 2, partners revisited the ideas and discussed them in more detail to streamline into more concrete potential research projects. It is assumed, given their engagement in the workshop, that they would like to pursue these research ideas and will suggest them in their proposals for round 2.

  Some anticipated challenges for the collaborative projects include partners may not be interested in collaborative project idea, different support may be required for conflicting interpersonal dynamics that may arise, and distributed nature of partners may make collaborative research difficult.

- **Identifying Team Leads -** As part of the research proposal for the collaborative research projects, partners must specify roles they would like to assume during project duration. Leaders may apply specifically to lead the research (or the CL may proposition them to lead the research). Team leaders will receive a slight increase in funding for this position. The assumption is that team leaders will need to do slightly more work than their research team, and thus additional funding will compensate for added responsibility. As one of the larger goals of the project is to slowly lift the reliance of the CL to maintain the network, and become self-sustaining, it is hoped that creating project leaders with help to transfer some leadership into the network and begin this transition. Some of the anticipated challenges include the risk that leaders may not self-identify and we will have to proposition partners to lead, partners will request playing the leadership role that are under qualified, or that project leaders may not fulfill the full scope of their duties.

- **Peer Review Board to Proposal Selection -** Proposals for the next round of funding will be selected with the support of an external peer-review group. They will be used to vet proposal and provide recommendations for which proposals should be funded. The assumption is that creating an external review board will help to mitigate perceived bias from the network regarding which partners are selected in the next round. The challenge will be to locate participants for the peer review board that are disconnected enough from the project but ascertain enough knowledge of the context to make educated decisions about proposal selection.

- **Integration of New Partners** - Little discussion has occurred around the process of integrating new partners into the network. It is unclear if and what efforts must be made. The network has begun to develop a trust and culture, and consideration should be taken on how to integrate new people. This is an area that should, ideally, be discussed during the proposal selection and approval phase.

- **Resiliency & Network Development -** Discussion between the PIUs and DECI mentors has raised interesting questions about the relationship of developing resilience to developing a network. Questions such as can developing resilience in a network actually develop a network? Can building resilience into networks be detrimental to disallowing networks that should fail from failing? Does resilience development start at the organizational level and transfer to the network level or vice versa? How does affiliation with the network impact level of resilience? What aspects of affiliation with the network build resilience? How is a resilient network defined? Is resilience a concept that network members deem important? Is this project networked enough to be considered a network for developing resilience? What is the capacity of the network to develop resilience? What support can and will partners provide? These questions will hopefully be answered in year 2 of the project.

C. Support / Capacity Building

Year 1 | Lessons Learned, Assumptions and Challenges

Capacity Building Exercises - during year 1 of the project, the CL provided a series of capacity building efforts to support partners. During CSN workshops, examples of sessions administered by the lab include Vision of Change, Theory of Change, Risk Management, Research Communications and Crisis Simulation. The opportunity was provided for partners to present their work and lessons learned so that partners could learn from one another. Workshop time was left open ended so that partners could self identify learning needs and/or areas they would like to discuss and collaborate on during the workshop. Travel grants were provided for partners to attend workshops beyond our own. Support was provided in the development of their reports and project deliverables. Support was also provided to help with the operations of their organization.

Areas identified by partners for support (Explicit)
CSN workshop 2 (Indonesia) - Partners requested support in the following areas: Knowledge sharing, Training, Research methodology, Collaboration, and Research topics and outputs. Research methodology requests related to privacy, governance, media, legal and social.

CSN workshop 3 (Toronto) - Prior to the workshop a pre-identified list of themes was developed using workshop 2 feedback and sent to participants. The objective of the survey was to gauge interest on the topics areas to help us design the workshop. Subject areas are listed from most requested to least requested below:

- Secure Network Communication & Knowledge Sharing
- Network Development (Goals, Objectives and Strategies) & Research Methodology
- Training & Material Design
- Organizational Resilience Development

Year 2 | Moving Forward

Peer mentors (Regional)- over the course of the project the idea has emerged to use peer-mentorship as a capacity building measure for network partners, as well as to identify potential new partners for the network. The idea is to have one peer mentor per region. Peer mentors will be Citizen Lab staff / contacts. In the past year, lab partner Christopher Gore served as a peer mentor for the Africa region in the past year, and worked with our African partners. His efforts were substantial yet some of the organizations did not perform as required even with his support. From his experience, we are moving forward with the assumption that the peer mentorship model will help build the capacity of partners and help them to achieve project deliverables in sufficient time and higher quality. This model was also helpful for the CL to use as an informal evaluation mechanism for assessing partner performance. It was also learned, that simply having a peer mentor does not imply organizational capacity will develop to a level that allows them to retain funding with the project.

Peer Mentors (Citizen Lab) - To contribute to capacity building, citizen lab staff have and will continue to work with CSN partners in areas they require support. During workshop 3, for example, the idea of applying the survey constructed by Chris Parsons to assess telecoms companies usage of private data in CSN partner countries was suggested on multiple occasions.

Upcoming workshops - Based on past feedback, and areas identified, the next workshops will continue to develop the research communication skills of partners. One of the ongoing challenges, is we are trying to bridge research with advocacy, yet most partners are not formal researchers. Thus, workshops should continue to build these skills. Workshops should be designed based on the specific nature of the proposals accepted, and areas identified where partners might need support. Ongoing Security exercises / resilience training will also occur.

Areas that need to be addressed / Ongoing Challenges

Secure communications - the need for secure communications has emerged from network partners, and the CL has developed a secure IRC channel for this purpose. Partners are not using it however. It is unclear why not. Ongoing discussion with the CSN is required, perhaps in-person discussion in the next workshop to see what other options are useful.

Needs during workshop vs. Post workshop are different - Another ongoing issue, is that in many cases, participants request certain support but after sufficient time has passed they are not longer in need of the support or it is not as crucial. We have used surveys to assess participant needs post / pre workshops, yet engagement in surveys is low. Prior to the most recent workshop, a series of 3 surveys were sent to the CSN with an incentive. Engagement seemed higher than normal on these surveys. In discussion with partners upon arrival at workshop 3, many of them said they completed the surveys simply because they wanted the incentive. Additional work is required in this area to identify how we can balance identified needs during and outside workshop times

D.**Maximizing Influence / Impact**

Year 1 & 2 | Reflecting and Looking Forward

Vision & Theory of Change

We used these activities to identify what exactly partners thought “influence” or “impact” looked like, so that we could qualify / quantify what exactly we are trying to support partners to achieve. They were driven by topics including: freedom of expression, cybercrime, privacy, Internet freedom, safety online, ICT policy change and broader human rights issues. Most of them were driven to create systemic change. To achieve these visions, they identified citizen empowerment, capacity building on digital rights and safety, developing global awareness. For a detailed analysis of these activities refer to UFE report 2. Moving forward additional work is required to identify a common vision and identify for the network. The assumption is that developing the research communications piece of the project might include further defining impact and help us work towards having a more concrete understanding of what impact looks ike.

E. Roles & Responsibilities

Year 1 & 2 | Reflecting and Looking Forward

CL vs. CSN Roles

Although the KEQ1 was worded to reflect a horizontal leadership structure between CSN partners and the CSN, as the year has progressed it is evident that the network has adopted a hub and spoke structure for most of it's dealings. Although we have tried to get partners to self-initiated and get the network transitioning to a self-sufficient network, the CL remains to be the main coordinator / connector for the network. It's hoped in the next year with continued relationship building, collaborative projects, and the identification of project leaders and eventually regional hubs that power can start to be distributed a little more evenly through the network

PART 3. KEQ3 Analysis

A. Objective

This section of the report aims to answer and provide reflections on KEQ 3:

- ***How can security and resilience be assessed and developed in a networked project?"***
    - *What is the role of the citizen lab, as a network facilitator?*
    - *What is the role of the cyber stewards, as network partners?*

Data will be analyzed from CSN workshop 3, outputs generated from this work will be described, lessons learned and recommendations will be provided associated with assessment and development of resilience.

B. Data Analysis

Data collected is analyzed under the following themes: defining & developing resilience, assessing resilience and resilience challenges.

Defining & Developing Resilience

Resilience Definition

As part of assessing and developing resilience, we wanted to establish a baseline definition for a resilient network. To do so participants were asked to define resilience in general. Key elements of their description of resilience is provided below:

Resilience includes elements of :

- Ready for the unexpected — ability to problem solve, backup plans
- Able to continue operations in an unstable environment e.g. funding changing, having backup plans
- Ability to bounce back after moments of instability

Organization / Network Resilience Development Attributes

They were then asked to define resilience in their organizational context i.e. distributed civil society organizations, and in a network. They were also asked how they perceived resilience to be developed in the both contexts. This data has been combined to yield a series of themes that describe the CSN participants perceptions of how resilience can be developed.

- **Internal affiliation** - Individuals and organizations achieve resilience simply through affiliation with the network. Resilient individuals and organizations are believed to contribute to the resilience of a network as well.
- **External affiliation** — Affiliate with many organizations or networks. If one organization goes down the network can work together to cover for it and help it recover. Affiliations can support and/or enhance reputation, credibility, safety and cause. Distributed situational awareness helps develop an early warning system. Partnerships with government / private sector must be regulated. Strong bonds or ties are required.
- **Shared vision and ideologies** — an organization with a sense of soul, with a shared vision and ideologies, is required to strengthen bonds and unite the organization or network
- **Diversification** — Diversify organization and network affiliations (at the organizational and network level). Partner with less vulnerable organizations to help lower overall risk and/or distribute risk throughout the network. Draw from multiple funders, and ensure they are not government or private sector.
- **Sphere approach** — Develop resilience by starting with smaller networks, or spheres, and move outwards. The perception is that smaller networks are more resilient. Spheres should be common spheres of work.
- **Plans & protocols** - Develop plans and protocols ahead of time to make knowledge explicit if an organization needs to continue without leaders. Identify memorandums of understanding for how to work together, common time zones, business, backup, long term, physical security, psychosocial security, network security, data storage, secure communications plans, etc.
- **Bottoms-up approach** — to developing plans, culture of resilience
- **Knowledge sharing** — information sharing; learning from failures and successes of others
- **Secure communications infrastructure -** to facilitate collaboration and knowledge sharing, as well as protect the sources that provide information the fuel the initiative
- **Psychosocial support** - provides empathy, support and inclusivity
- **Contacts pre-established** - Network requires legal, security, technical contacts established ahead of time
- **Mutually beneficial / symbiotic relationship** - members must experience feel a mutually beneficial relationship with the network
- **Decentralized decision making** — horizontal / decentralized leadership is required to allow spheres to operate freely with little dependency on approval process

Assessing Resilience

Resilience was assessed using a survey developed by Resilient Organizations (2013) that asks users to rank 13 indicators of a resilient organization, which combine to develop a resilience score from low to high organizational resilience. This tool was sent to all stewards, with six replies received, five being from stewards. Resilience scores were calculated, and follow-up interview / focus groups were completed with each of the stewards that completed the survey.

Status of Organizational Resilience in CSN Member Organizations

Partners were asked for their perceptions of their organizational resilience and also assessed using the survey. One organization classified themselves as not resilient, one as resilient, and the remainder somewhat resilient. The survey results were similar. Cyber Stewards organizations (in one case an individual) ranked as follows: one low, two medium and two high organizational resilience. Qualitative discussion revealed stewards are not prepared for the unexpected. They lack of awareness of threats, security standards are low, and no contingency plans are in place. One organization stated they have low understanding of encryption and often face successive crises but lack the resources to learn from them. Another two organizations mentioned that they rely too heavily on the "front men" to run the organization. Others that felt they were somewhat prepared, also experience ongoing crisis but felt that it helped them sustain a continual state of readiness. The indicators that ranked high from the survey reflects members are strong at relationship building, they buy into emergency planning, and exhibiting perseverance for problem solving in a crisis. One member stated that resilience was all about resources, and if you have no resources you have nothing to lose. For a detailed analysis of challenges and strategies to develop resilience in these organizations and in larger networks see section C.

The Assessment Tool

There was also discussion about the tool itself, which is described below:

- *Usefulness* — participants found the survey useful. It helped users think more about the notion of resilience short-term and long-term, and shed light on the aspects of resilience I.e. reputation management, and organizational priorities. One respondent said they survey made them feel more prepared than they thought.
- *Actions taken* — None of the stewards took any follow-up *actions* as a result of the survey, however they expressed interest in learning more and the desire to have access to the tool to share with their own organizations.

Challenges with Assessing Resilience

There were challenges associated with assessing resilience identified. Participants felt that their distributed nature makes it difficult when people are not physically together. This implies resilience is really being assessed at the individual level.

Challenges with Developing Resilience in Networks

Data collected from the definition, identification of developmental indicators and assessment of resilience yielded the following challenges faced by organizations that are distributed into networks like the CSN:

Organization Specific

- State of surveillance and information controls — Situation monitoring is difficult in countries that are heavily regulated e.g. inside Tibet
- Insufficient backup staff — there are people that can step up to lead, but not as well trained / knowledgeable
- Transforming NGO Reputation — Organizations grow quickly and image of organization transforms i.e. organization that starts out as a media organization quickly transitions to an advocacy organization which assumes heightened risk
- Insufficient resources - resources required to plan, train and equip for the unexpected
- Limitations of donor funding — when operating from donor funding specific to a project, difficult to allocate resources to resilience measures and/or save for future
- Culture of country — countries with complex risk (political, economic, environmental, etc.) impacts capacity for resilience
- Perception of NGO — a poor perception can increase risk / decrease resilience
- ICT Vulnerabilities — Infrastructure can never be 100% secure

Network Specific

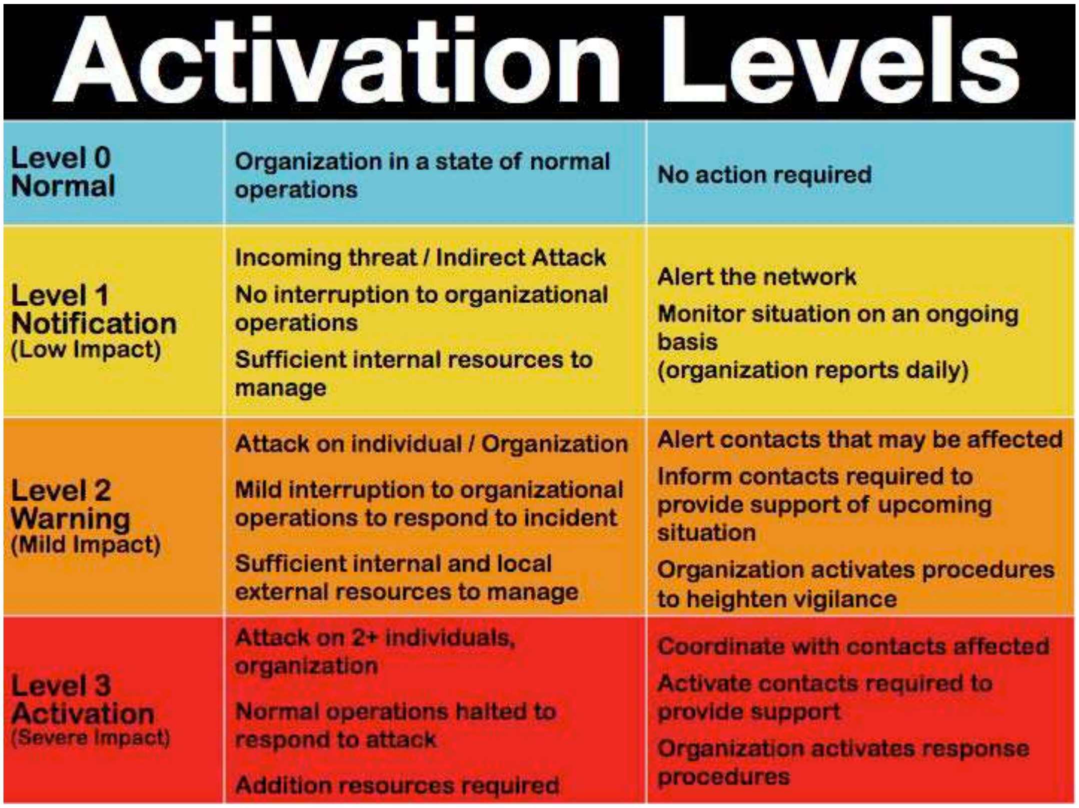
- Distributed nature / multiple time zones — Decision making is difficult when people aren't physically together — issues with time zones, inability to discuss in a timely fashion, lack dynamics of discussion, some decisions must be made with some people missing
- Decreased ownership — Low sense of ownership within a network
- Horizontal versus vertical — Networks can be too centralized or too horizontal which can be tough to find a balance
- Member protection — Need to protect the voices to send out the message; ensure a campaign does not endanger members revealing unsolicited sensitive material
- Collaboration can be difficult — in contexts like the CSN, members are all working on different things, they are very independent / don't work together

C.Outputs & Interventions

In addition to research findings, some of the data collected will be used to contribute to outputs including a) activation levels and b) Standard Operating Procedures (SOPs), and interventions.

Activation Levels

Prior to the emergency simulation, a first draft of Activation Levels was developed for pilot during the simulation (see Figure 1)



Activation Levels		
Level 0 **Normal**	Organization in a state of normal operations	No action required
Level 1 **Notification** (Low Impact)	Incoming threat / Indirect Attack No interruption to organizational operations Sufficient internal resources to manage	Alert the network Monitor situation on an ongoing basis (organization reports daily)
Level 2 **Warning** (Mild Impact)	Attack on individual / Organization Mild interruption to organizational operations to respond to incident Sufficient internal and local external resources to manage	Alert contacts that may be affected Inform contacts required to provide support of upcoming situation Organization activates procedures to heighten vigilance
Level 3 **Activation** (Severe Impact)	Attack on 2+ individuals, organization Normal operations halted to respond to attack Addition resources required	Coordinate with contacts affected Activate contacts required to provide support Organization activates response procedures

Figure 1. Activation Levels

During discussion of the scenario, we discussed the application of this table to the CSN context. Notes taken from this discussion will be combined with the data collected from Survey 2 - Security Protocol Development to revise this table and tailor more specifically to the needs of the CSN members.

Security Protocol Document

Prior to the simulation, a first draft of the security protocol document was developed (see Annex I) and later distributed to CSN members for pilot during the simulation. Comments on the tool combined with data collected Survey 2, will be used to modify the draft.

Interventions

A series of ideas for interventions to facilitate the assessment and development of security and resilience emerged in the last workshop, and are outlined as follows:

Resilience Working Group (RWG): The aim of the RWG is to develop a voluntary sub-network of the CSN that will be co-creators in this research, and also leaders for the assessment and development of resilience in the network. Working with a sub-group will mitigate the risk of losing participants, facilitate deeper buy-in and engagement in the process, provide closer insight into the needs of the larger network, and mitigate challenges associated with meeting scheduling across multiple timezones. It is anticipated that using an RWG will facilitate building capacity in the external network, as well as internally.

Virtual Debriefs: a process of gathering individuals within or across organizations to share their experiences about how their organization responded to an event so that lessons learned can be identified; they encourage learning, foster trust building, and facilitate information gathering and forward planning. During or after a CSN partner experiences an event, a CSN virtual debrief would be scheduled to discuss and learn from the event.

Table-tops (Virtual, Face-to-Face): "…facilitated discussion based activities in which participants review and explore the response to a specific emergency scenario, but do not perform and actions" (Public Safety, 2013, p3). They use real-scenarios, and situation updates, or injects, delivered to participants over a specific timeline designed to emulate how a crisis would unfold. They will be used to reverse engineer and test plans, roles and responsibilities.

D.**Lessons Learned**

The concept of "Resilience"

- *Resilience is a foreign concept* — in participant interviews, combined with observations during workshops around risk and emergency simulation that were provided, most participants were unfamiliar with the concept of organizational resilience
- *Difficult to distinguish between a resilient network and organization* — indicators provided that define a resilient organization or network were similar; the way these indicators manifest is different
- Distributed organization versus network — difficult to distinguish / some confusion

Assessing Network Resilience

- *Tool needs modification* — although partners found the resilience assessment tool useful for helping them think more about, and understand resilience, it was felt the tool needed to be tailored for their context I.e. it was too corporate. Participants thought the survey needed to cover more about assets at digital risk (e.g. Technologies including hardware, data, communication channels, etc.). They also felt that the survey seemed to be targeted to corporate or larger organizations. Doesn't account for aspects unique to their context e.g. Distributed nature, reliance on technology, reliance on funders, unique risk context.
- *Desire to assess resilience within their organizations* — partners wanted the opportunity to use the tool, either existing or modified, with their own organizations to assess their colleagues perceptions around resilience; seen as a resilience building measure
- *Questioning the need for consistency in perceptions of resilience* - one participant mentioned that they didn't know how their perceptions of resilience in their organization aligned with others — the question emerged, is this a good or bad thing? To what level should an organizations' perceptions of its resilience be consistent?
- *More emphasis on assessment* — need a way to assess a baseline of emergency preparedness of an organization

Developing Network Resilience

- *Difficult to develop resilience* — participants were either either a) unfamiliar with the notion of resilience b) aware of the concept but not on the radar of the organization and c) perceived need for a culture of resilience but lack of resources to develop
- *Important but not THAT important* - participants felt that resilience was a concept that was important (some more than others) but felt that there were bigger priorities to address
- *Where do we begin?* — There was mixed opinions around whether a resilient network is developed because organizations are resilient, whether organizations can develop resilience because a network is resilient, whether developing resilience is neither about the organization or network it's about the nature of the nodes, or resilience starts at the individual level;
- Resilience development indicators - Aspects raised in DECI discussion around the development of resilience in networks are outlined in Table 1.

Table 1. PIU Questions about Resilient Networks

THEME	QUESTIONS RAISED
Notion of Resilience in Networks	Does the network need to be resilient? When does it need to be and not? Why is it important?
Nature of the network	Homogeneity Size Network design - How does a resilient network model look for different models of networks I.e. CSN is a hub and spoke network?
Generalizability	Applicability to other networks — how does what we are trying to develop translate to other networks
Relationships	Solidarity — thematically consolidated; how would you distinguish a cyber solidarity network The ties that bind a network — is this a family network or supporter?
Role of Research	CL provides research to support partners — to what extent is this developing resilience? How does research bridge with advocacy?
Role of Affiliation	Could discuss with Tibet Action Institute — how did working with the CL help them? To what extent does affiliation with developed world / academic institutions (in terms of advocacy networks) relate to the development of resilience? What is the role of partners to the existing network?
Assessment / Measurement	How is resilience measured in differently in different contexts?

Roles & Responsibilities

- *Need to identify* — participants expressed desired to collaborate and support one another in a crisis, yet didn't know their role / responsibilities. The need was expressed to define these roles and responsibilities
- Capacity for response — in addition to roles and responsibilities, there is the ongoing question of the network's capacity to respond / provide support I.e. This is an advocacy network that does research — to what extent does it need resilience? And what support can partners offer one another in terms of crisis response?

E. Recommendations

Drawing from feedback from the CSN and PIUS the following recommendations can be made for KEQ3 in the second phase of the project. List is provided in order of priority from high to low.

- Develop Resilience Working Group
- Customize the resilience assessment tool specific to the CSN context & distribute to partners for them to share with their own organizations; use their feedback in implementing the revised assessment tool to revise further and/or contribute to understanding of how resilience is developed
- Complete Security Protocol / SOPs
- Run Virtual debriefs
- Virtual simulations

PART 4. UFE Lessons Learned

A. Implementation

The UFE process was initiated in Sept 2013. Two full iterations of the process have been completed to-date. The project timeline in correlation of the 12-step process identified by Broadhead & Ramirez (2013)[2] is as follows:

Step 1 - 8	September to October 2013
Step 9	October 2013
Step 10 - 12	October to December 2013
Step 5 - 7	January to April 2014 (Step 8 - simulation of use step skipped)
Step 9	April 2014
Step 10 - 12	May to November 2014

Drawing from their UFE model, an outline of how the project was implemented can be seen in Figure 2. This diagram also outlines the specific actions taken within each step of the process, and how meetings aligned with points of the process. Note, a diagram was developed for the first part of the process only since the cycle is iterative.

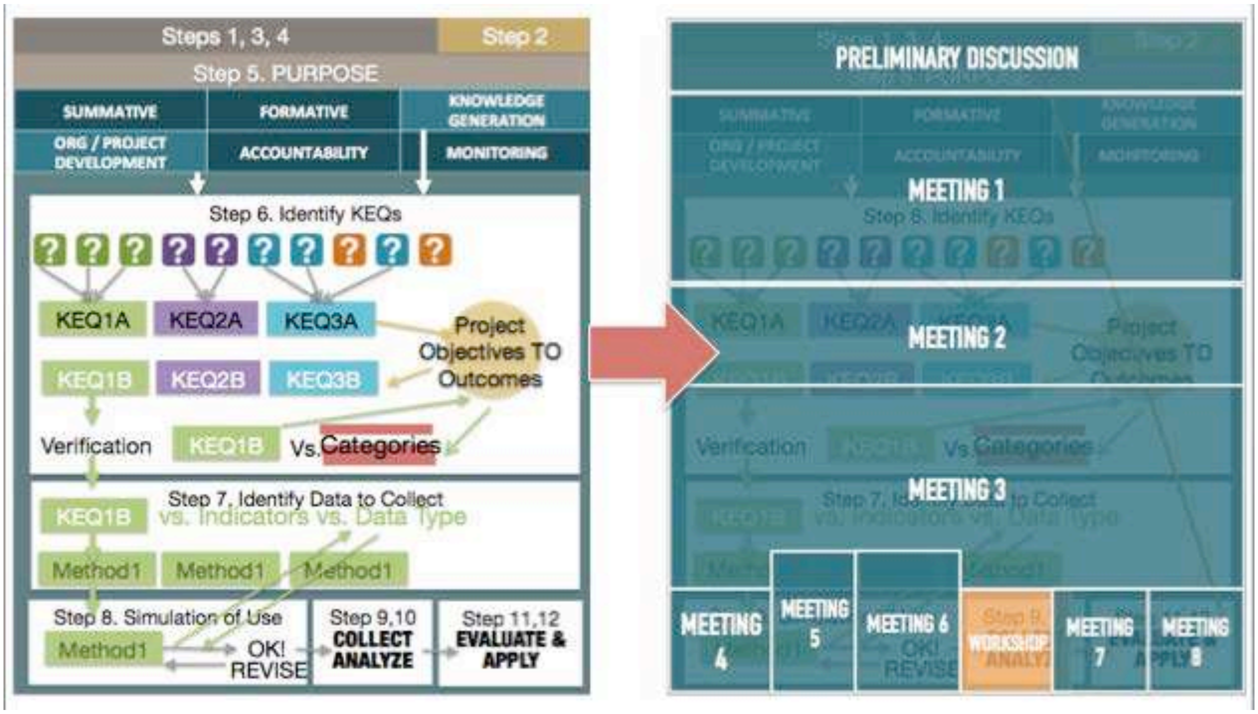


Figure 2. UFE Process

[2] Ramirez, R., & Broadhead, D. (2013). *Utilization Focused Evaluation: A primer for evaluators* (pp. 1–132).

B. Successes

Aspects of UFE application that *benefited* the project include:

UFE Process

- **UFE was a learning process** — helped us step back and identify we were not actually developing a network / made us rethink the notion of network
- **Buy-in essential** — buy in from the funder (IDRC), the primary organization (Citizen Lab) and CSN members helped to progress the project from the ground up using the linear UFE process step-by-step

Steps in the process

- **Focus on use** — helped us identify how exactly the evaluation would suit our needs
- **KEQ identification** — helped us to identify our priorities for developing CSN capacity and the larger network
- **Project objectives** - forced us to clarify our project objectives which helped us to plan our approach and subsequent capacity building activities and interactions with the network
- **Project outcomes vs. Impact** - understanding the distinction between planning for outcomes instead of impacts (a variable more difficult to measure) we tailored our KEQs closer to tangible results
- **Data identification** — helped us ensure the questions we'd like to ask were answerable, the many different types of data / approaches to answering our questions, and provided insight into the tools we could use to collect the data and subsequently also build capacity
- **Simulation of use** — although brief, was useful to help us identify a) any usability issues associated with the tools we selected for data collection, and b) tools would select the type of data we are looking for

DECI / Mentor interaction

- **Knowledge transfer / lessons learned** — provided advice / solutions to problems drawing on experience using UFE, much of this knowledge being difficult to explain through text
- **Sped up the process** — through his support we were able to distribute the learning between the evaluator and the mentor, allowing the evaluator to just draw on the experience of the mentor to help us move through the process instead of having to "learn as you go"
- **Prevented mistakes** — I.e. KEQs, the mentor helped us identify aspects of the KEQs we identified in the early stages that could cause problems further down the road
- **Tools & strategies** — knowledge of strategies and tools to work with PIUs and CSN members to link to our KEQs. Examples include the activities suggested

for each of the KEQs we wished to touch on in the CSN workshop 2 in Bali, Indonesia; also provided useful activities for streamlining KEQs that otherwise would have been a daunting task

C. Challenges

Aspects of UFE application that were *challenging* include:

UFE Process

- Simulation of use — given time constraints, we didn't have the opportunity to use the simulation of use step to it's fullest potential
- UFE round 2 bit unclear — After the first workshop, it was a bit unclear how the UFE process would continue.. After I put out the first report we talked about the findings,
- KEQ1 too abstract — although we saw value in KEQ1, as the project progressed we felt this question, although useful, was not linked closely to the actual work that had to completed with the CSN. In turn, emphasis was placed on KEQ2 and 3 for the remainder of project.

Project Challenges

- UFE was resource heavy — the UFE project required one person specifically designated to UFE. As the CSN was run by two other part time staff members, some of the time allocated to UFE by the third staff member would have been more useful if dedicated to the administration of the project.
- Avoid the word evaluation — given power dynamics were of concern between the CSN and the Citizen Lab, the PIUs felt it was important to not use the word evaluation when introducing the project. As a workaround, we titled the project Collaborative Learning Initiative.
- Link between ResComms was unclear — although we tried to bridge ResComms and UFE aspects of the project, it felt like the work was done separately and the bridge between the two is still unclear

Workshop Design & Data Collection

- Competing workshop priorities — It was difficult to allocate sufficient time to UFE in the workshops given reporting requirements and need to provide open time for partners to collaborate
- Remote data collection difficult — It was difficult to collect data remotely due to low engagement of partners. For example, 4 partners out of the full network successfully completed all three of three surveys pre-CSN workshop 3 (with incentive provided)
- Workshop 1 was over planned — too many activities planned and not enough time
- Data collection and analysis time consuming — a lot of data was generated from small activities in the workshops, and analysis was quite time intensive

D.UFE Impact

The application of UFE had the following impacts on the design and implementation of the project:

- **Design of CSN workshops -** Using the UFE process and KEQs we were seeking to answer, combined with the support of mentors, working with UFE helped us design workshops that used a participatory approach, provided time for partners to discuss and troubleshoot their own projects, and encourage group work. Participants enjoyed this format, and felt that our workshop format was different, more interactive and user-focused.
- **Need for secure communications —** One of the findings from our KEQs was that participants requested secure communication channels. We are currently in the process setting up this capacity.
- **Need for collaboration —** In the Bali workshop, participants requested the opportunity to work together further in one of the activities and developed ideas for collaborative projects. We designed the next workshop and the next project phase to integrate collaborative research projects based on this finding.
- **Need for risk awareness -** In the Bali workshop, running a risk assessment exercise with participants revealed they had minimal experience in thinking about and managing risk. Once we taught them how to think about risk, more desire was expressed to learn more and some partners have begun integrating this training into their own work
- **Emergency Management materials being re-used —** more than one participant have reported using the approach and materials provided in the risk segment of the CSN workshops in their own trainings e.g. Tibet Action Institute now teaches the risk matrix.
- **Need for network resilience —** In the Toronto workshop, discussions during the emergency simulation revealed that partners a) need support in a crisis due to lack of resources and b) networks members wished to have the opportunity to provide support. Gaps e.g. Roles and responsibilities, as well as activities and tools to develop resilience were identified and will be developed / implemented in subsequent workshops
- **Findings used in reports —** Data collected and analyzed in UFE has been used for populating other reports e.g. IDRC reports

E. Recommendations

Key Evaluation Questions

The following is a summary of recommendations for the KEQs. For detailed recommendations for KEQ1 and 3, refer to Part 2 and 3 of this report.

KEQ1: How can network partners support one another to maximize influence and impact at their local, regional, and/or international level? *What is the role of the citizen lab, as a network facilitator? What is the role of the cyber stewards, as network partners?*

Data collected for this question is around enhancing collaboration and improving impact. Partners identified collaborative projects as a means to enhance collaboration and create better research. Ongoing meetings helps to build trust and collegiality between partners, as well as foster ideas. Discussions about security and risk helped partners to reflect on their current operational practices and how to start operating in a safer, more secure manner. A mission statement helped to generate a common vision, yet draw little engagement from partners.

Although this question hasn't yielded a finite answer, during the project this question was deemed less important than the others. This was because KEQ2 and KEQ3 were thought to be more directly linked to the immediate needs of the project.

KEQ2: How can communication be improved between network partners for the sharing of skills, knowledge, tools, etc.?
What is the role of the citizen lab, as a network facilitator? What is the role of the cyber stewards, as network partners?

Although the focus of this report is not on KEQ2, the ResComms piece of the project, observations from the UFE perspective of the project show that implementation of secure communication channels, ongoing in-person meetings, frequent use of the CSN mailing list, and ongoing training on communication strategies (like the workshop delivered by Ricardo from DECI in the CSN Workshop 3) will facilitate improved communication.

More work is required for this question, yet the question could be narrowed to target some of the more specific communication related needs at this stage of the project.

KEQ3: How can security and resilience be assessed and developed in a networked project? *What is the role of the citizen lab, as a network facilitator? What is the role of the cyber stewards, as network partners?*

Drawing from the data presented in Part 3, preliminary research shows that assessing resilience using the tool developed by Resilient Orgs (2013), designed for NGOs was useful but not tailored specifically to the needs of networks like the CSN. Partners perceived resilience is developed using a bottoms-up sphere-like approach, where decision making is decentralized, plans, procedures and contacts are pre-established, membership is diversified. affiliations are with internal and external organizations and networks, relationships are mutually beneficial; and a culture of knowledge sharing, shared ideologies, and psychosocial support. Challenges that emerged around the development of resilience, however, ranged from organization specific ones including insufficient resources, context specific surveillance and information controls, and donor imposed restrictions. and network specific challenges including distributed decision making, low ownerships, member protection, and distributed collaboration. The role of the citizen lab and cyber stewards network, at this point, is unclear, yet the need was expressed to identify roles and responsibilities to facilitate future collaboration.

Additional work is required to a) identify a custom tailored solution to assessing resilience b) further assess approaches for the development of resilience c) build capacity around indicators identified that are linked to the development of resilience and d) develop mechanisms to mitigate the challenges associated with the development of resilience.

Future Areas for UFE Evaluation

Given we are moving into Phase 2 of the project, the UFE process could be used to evaluate more specific elements of the CSN project. Some thematic areas that have emerged for development include:

- *Assessing impact* — Partners had a difficult time in their reports assessing and reporting on impact
- *Improve research capacity* — Although a primary function of the CSN is to develop research, it came out that partners need to learn more about the process of conducting and writing quality research
- *Facilitate reporting practices and procedures* — Partners have multiple reporting requirements and thus find it difficult to meet the reporting requirements on time that we needed
- *Improve cyber security knowledge* — Partners want to build capacity around cyber security
- *Develop resilience* — Although partners deem other aspects of their work higher priority, ongoing work with the stewards to start building a culture of risk

awareness and resilience has started to create the buy-in to engage in the emergency preparedness and further resilience development activities

- *Develop network sustainability* — Although we have gone to great measures to develop a network, it is uncertain at this point on whether the network could / would sustain itself without the Citizen Lab's involvement. Next stage of KEQs should focus on sustainability.
- *Enhance collaboration between partners* — In the second workshop, the idea for collaborative projects emerged with great enthusiasm; this idea was pushed forward in the third workshop, and participants were still keen to contribute. Following this workshop, however, momentum was lost on the research project ideas and little engagement has been observed on these ideas

Future Applications of UFE

In the next stages of the project, a few recommendations that could be made for the application of UFE include:

- *Streamline UFE reporting requirements with IDRC* — multiple reports were required during the project that were separate from UFE reports. It might be useful, when planning UFE, to start at the end of the project and work backwards. Look at the deliverables, reporting requirements, etc in more detail and plan to UFE so that it's used as an evaluation but as to facilitate the progress of the project, and more specifically facilitate the completion of donor reports.
- *Build relationship between ResComms and UFE* — although we tried to bridge UFE and ResComms through selecting one KEQ that was specifically ResComms, both elements were completed seemingly in isolation of one another. Perhaps future iterations of UFE could use one person that does both UFE and ResComms, or perhaps KEQ could be developed that draws on both ResComms and UFE
- *Develop greater baseline understanding of the UFE process from the beginning* — although we had a rough idea of UFE, there were some scepticism around the use of UFE and confusion around the purpose. In hindsight the process is more apparent, however in the beginning it might have been useful to have a more concrete layout of the UFE process, the tools and specific approaches that would be integrated as a means to enhance understanding.

Conclusions

This report was designed to summarize data collected in the most recent workshop (Toronto, ON) as well as to reflect on the UFE project and provide recommendations for the next phase of the CSN project and similar projects. Drawing from the findings and lessons learned from using the Utilization Focused Evaluation approach to evaluate our CSN project, the UFE process has been proven useful for initiating and progressing the project. Designing UFE in the next phase of the project with the administrative / operational requirements of running the project central to the design, it is recommended to continue adopting a UFE approach to the development of such projects.

Annex A. Agenda

Sunday March 30

8:00-10:00 AM CSN Partner Breakfast

Park Hyatt Hotel
Prince Arthur Ballroom

For the CSN partners we have organized a welcome breakfast at the hotel on Sunday morning. We will start at 8am but you can drop in until 10am.

Cyber Dialogue Agenda can be found here: http://www.cyberdialogue.ca/2014-agenda/

CSN Workshop Preparation

Project Progress Presentation

Each CSN partner will give a 10 minute presentation on their project progress that answers the following questions:

- What are your achievements and milestones so far in your project?
- What have you learned from the project so far?
- What struggles have you encountered with this project / your work in general?
- What do you need help with?

Research Communications

As a preparation for this session please fill in this survey here https://canadacentre.wufoo.com/forms/cyber-stewards-network-research-communications/ and bring examples of materials you use for communications to the workshop (e.g. send links to websites, videos, documents, flyers brochures and other printed materials, etc)

Shahzad and Ramiro: *Research / Advocacy and Public Litigation*
Donny and ‘Gbenga: *Research / Advocacy and Public Policy*
Olga and Lobsang: *Research / Advocacy and Community Outreach*

Each of these presentations will address the following questions:

1. What was the problem you wanted to address?
2. What (policy / social) change did you want to bring about?
3. What action(s) did you undertake and what alternative actions did you consider, if any?
4. What was the result?
5. What worked well and what didn't?

Break out group proposals

If you have a breakout group suggestion you want to make before the workshop please fill in the form here: https://canadacentre.wufoo.com/forms/csn-workshop-sessions/

For a list of breakout groups that have been suggested so far see here: https://canadacentre.wufoo.com/reports/csn-workshop-suggestions/

CSN Workshop Agenda

Tuesday April 1: Day 1

Location: Hart House, South Dining Room
7 Hart House Circle
http://harthouse.ca/maps-directions/

8:30 - 9:00 AM Breakfast

9:00 - 9:30 - Welcome

- Introduction to workshop objectives and agenda
- Materials and process
- Lighting Intros for new participants

9:30 - 10:30 AM - Partner Project Updates and Discussion
During this session we will update each other on our project progress and address the following questions:

- What have we achieved so far?
- What challenges have we encountered?
- What can we do to help each other?

10:30 - 10:45 - BREAK

10:45 - 12:30 Partner Project Updates

12:30 - 1:30 Lunch

1:30 - 2:00 - Introduction to Research Communications
- Ricardo Ramirez (DECI)

2:00 - 3:30 - Research Communication and the CSN

Shahzad and Ramiro: *Research / Advocacy and Public Litigation*
Donny and ‘Gbenga: *Research / Advocacy and Public Policy*
Olga and Lobsang: *Research / Advocacy and Community Outreach*

3:30 - 3:45 - BREAK

3:45 - 5:00 Review Day 1 and Plan Day 2

Dinner on your own.

Wednesday April 2

Location: Hart House, South Dining Room
Breakout room: North Dining Room
7 Hart House Circle
http://harthouse.ca/maps-directions/
8:30 - 9:00 AM Breakfast
We propose using day 2 to discuss the collaborative project ideas we developed during our Indonesia workshop.

Project descriptions are posted here: https://docs.google.com/document/d/1rgtO1UnRMK24D9XgJGUIS5ad9mapKdUGU28vNsl3yjk/edit#

9:00 - 9:15 Organize into working groups

9:15 - 10:30 Breakout Groups

10:30 - 10:45 - BREAK

10:45 - 12:30 Breakout Groups

12:30 - 1:30 Lunch

1:30 - 3:30 - Breakout Groups

3:30 - 3:45 - BREAK

3:45 - 5:00 Review Day 2 and Plan Day 3

Dinner on your own

Thursday April 3: Day 3

8:30 - 9:00 AM Breakfast

9:00-9:15 Welcome and Introduction to Day 3

9:15 - 11:30 Security Exercise

For the first half of the morning we will run a table-top exercise to test the first draft of the Security Protocol document we've developed for the network.

Participants will run through a simulated crisis and be prompted to respond to each phase using the protocol and one another.

11:30 - 12:00 Plan breakout groups for afternoon

12:00-1:00 LUNCH

1:00 - 4:00 Breakout groups / Open

The schedule for day 3 is left open for breakout groups and other activities we can generate during the first two days.

To suggest a session ahead of the workshop please use this form: https://canadacentre.wufoo.com/forms/csn-workshop-sessions/

4:00 - 5:00 Wrap up and Next steps

7:00 Group dinner

Annex B. Survey 1 – Planning Survey for Workshop 1

WORKSHOP PLANNING

The following questions will be used to guide the design of the upcoming workshop so that we may help you meet the deliverables of your projects

Identify and rank 5 of the following potential workshop areas for the upcoming workshop from 1st to 5th choice:

- Network Development - Goals, Objectives and Strategies
- Secure Network Communication & Knowledge Sharing
- Organizational Resilience Development
- Research Methodology
- Training & Material Design
- Other

If you specified OTHER, please describe:

LESSONS LEARNED FROM WORKSHOP 1

The following questions will be used to evaluate the previous workshop and help us plan the next workshop

1. What did you like about the last CSN workshop? Please provide at least 2 things
2. (Optional) What do you think could have been done differently at the last workshop to make it more engaging and/or productive?
3. How do you think we can build on what we learned from the last workshop for planning the next workshop in March 2014?
4. (Optional) How do you think being part of the CSN will help you do your work on the ground?
5. What is the unique contribution that this network could make to help its members in their work?

Annex C. Survey 1 – Data Analysis

Previous Workshop Evaluation
Participants liked the following about the last workshop:

- Goal setting for the CSN
- Discussion about research methodology
- Knowledge sharing on current projects / work
- Morning circle debriefs
- Participatory approach to workshop design
- Diversity of skills between participants
- Creative / innovative delivery of workshop
- IGF discussion
- Interactive / group discussions

Could have been improved:

- Allow each steward to provide an individual presentation to pose questions / problems
- Access to presentations and documents provided in workshop after the workshop
- Less time on disaster training
- One facilitator not two
- Different room format - no “board room” table
- More time for small group work / collaborative planning
- Better planning for time allotted

Next Workshop Planning
Participants indicated they wanted areas to be covered in their subsequent workshop in order from highest to lowest:

- Secure Network Communication & Knowledge Sharing
- Network Development - Goals, Objectives and Strategies
- Research Methodology
- Training & Material Design
- Organizational Resilience Development

Aspects to be integrated into the next workshop

- More sharing of lessons learned and opportunity for peer-feedback
- Substantive discussion on key issues faced by the stewards
- Material provided in advance
- Design a curriculum for the batch of cyber stewards meetings
- More interactive partner presentations
- More time for working groups
- Pursue the research ideas generated and ideas for collaborative projects

- **CSN Development**

Ways CSN currently contributes to support work on the ground

- Funding provides opportunity to attend conferences and study courses
- Expands network of potential collaborators / contacts
- Helps increase visibility of issues specific to a region
- Support for advocacy activities
- Introduces different advocacy strategies
- Builds capacity around the management of risk
- Provides research to build on the ground case
- Increases awareness of events around the world

Ways CSN could enhance support for work on the ground

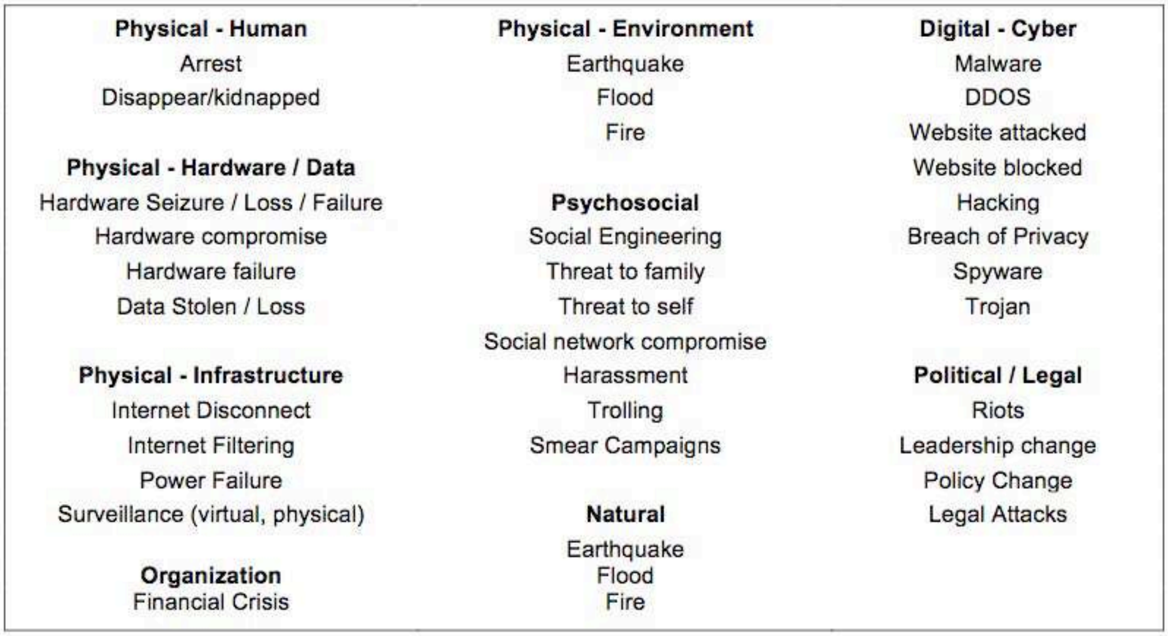
- Provide more insight into issues being addressed by the network
- Mentorship on how to build credible, legitimate and valid evidence targeted to policy makers
- Enhance collaboration
- Build more sustainable, secure ways of communication
- Increase visibility
- Provide high quality research
- Additional funding and research resources
- Collaborative project as a network e.g. Network-wide project on censorship

Annex D. Survey 2 – Security Protocol Development

INSTRUCTIONS

To complete the survey, do the following:

1. The table below is a list of all risks Identified in the past CSN workshop. Using this list, **identify 3 risks** that are **most likely** and **highest impact** for your organization.



Physical - Human
Arrest
Disappear/kidnapped

Physical - Hardware / Data
Hardware Seizure / Loss / Failure
Hardware compromise
Hardware failure
Data Stolen / Loss

Physical - Infrastructure
Internet Disconnect
Internet Filtering
Power Failure
Surveillance (virtual, physical)

Organization
Financial Crisis

Physical - Environment
Earthquake
Flood
Fire

Psychosocial
Social Engineering
Threat to family
Threat to self
Social network compromise
Harassment
Trolling
Smear Campaigns

Natural
Earthquake
Flood
Fire

Digital - Cyber
Malware
DDOS
Website attacked
Website blocked
Hacking
Breach of Privacy
Spyware
Trojan

Political / Legal
Riots
Leadership change
Policy Change
Legal Attacks

Figure 3. List of Risks

FOR EACH RISK

2. What is the risk? --> Select the risk name from the dropdown

Example: Pandemic

FOR EACH LEVEL

3. How do we know what activation level we are at? --> Describe triggers.

Triggers are used to define the activation level. They can be described considering the severity an individual and/or organization is impacted, the number of people affected, the resources required to be able to respond, how quickly action must be taken, etc.

4. How can we, the Citizen Lab / CSN support you? --> Identify the support required for each level

Example of Levels, Triggers and Support Reqd

LEVEL 1 - LOW IMPACT

Triggers:
3 employees in the organization have started showing symptoms of the virus but are able to continue work as normal; the situation must be monitored but no action is required; no additional resources required

Support required:
Alert partners of the situation, No support required

LEVEL 2 - MEDIUM IMPACT

Triggers:
Level 2 - Half the organization is affected with 25% staff hospital bound and 25% expressing symptoms; productivity in the workplace is diminished to 50%, additional resources required from local NGOs

Support required:
Solicit some help from partners to help identify the virus and mitigate the spread, to alert other partners of the risk, to help the organization perform basic functions

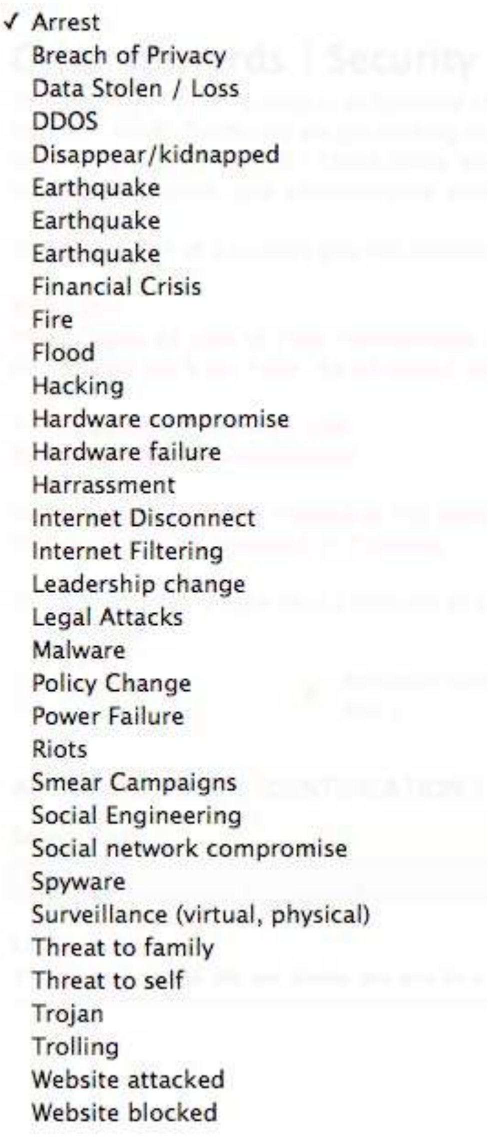
LEVEL 3 - HIGH IMPACT

Triggers:
The entire organization is affected with 60% hospitalized, 35% still coming to work but expressing symptoms; additional resources are required beyond the capacity of the local region as other NGOs are also under-resourced; action must be taken immediately to maintain operations while also protecting remaining staff

Support required:
Solicit immediate help from partners to help response to the situation, protecting remaining staff, removing the virus from the organization, building local capacity to perform critical organizational functions, communication and coordination of response groups, and facilitating recovery

ACTIVATION LEVEL IDENTIFICATION | RISK 1*

Select Risk from the drop down menu: (See Figure 3 for options)



✓ Arrest
Breach of Privacy
Data Stolen / Loss
DDOS
Disappear/kidnapped
Earthquake
Earthquake
Earthquake
Financial Crisis
Fire
Flood
Hacking
Hardware compromise
Hardware failure
Harrassment
Internet Disconnect
Internet Filtering
Leadership change
Legal Attacks
Malware
Policy Change
Power Failure
Riots
Smear Campaigns
Social Engineering
Social network compromise
Spyware
Surveillance (virtual, physical)
Threat to family
Threat to self
Trojan
Trolling
Website attacked
Website blocked

LEVEL 1
Trigger(s) - How do we know we are in a level 1 activation level?
Support Required from Network / Citizen Lab

LEVEL 2
Trigger(s) - How do we know we are in a level 2 activation level?
Support Required from Network / Citizen Lab

LEVEL 3
Trigger(s) - How do we know we are in a level 3 activation level?
Support Required from Network / Citizen Lab

*Note: This section was provided three times for three risks

Annex E. Survey 3 – Resilience Assessment Tool

RESILIENCE ASSESSMENT

The following assessment has been extracted from "A Short Guide To Resilience for NGOs" developed by The ResOrgs group in New Zealand.

The responses from this survey will be used to guide discussion about resilience in the workshop.

To what extent do you agree or disagree with the following statements for your organization?
(Rank between: Strongly Disagree, Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree, Strongly Agree)

- There would be good leadership from within our organisation if we were struck by a crisis
- People in our organisation are committed to working on a problem until it is resolved
- We proactively monitor our industry to have an early warning of emerging issues
- We can make tough decisions quickly
- We are known for our ability to use knowledge in novel ways
- We build relationships with others we might have to work with in a crisis
- If key people were unavailable, there are always others who could fill their role
- There are few barriers stopping us from working well with other organisations
- Our organisation maintains sufficient resources to absorb unexpected change
- We have clearly defined priorities for what is important during and after a crisis
- We have a focus on being able to respond to the unexpected
- Given our level of importance, I believe the way we plan for the unexpected is appropriate
- We believe emergency plans must be practised and tested to be effective
- Describe how this survey aligns with the risk context of your organization
- (i.e. does it miss any areas? talk about areas that don't apply to you? does it address all areas?)

Annex F. Survey 3 – Data Analysis

The resilience survey developed by Resilient Organizations (2013) ask users to rank the following criteria from Strongly Disagree (score of 0) to Strongly Agree (score of 7 points):

1. There would be good leadership from within our organisation if we were struck by a crisis
2. People in our organisation are committed to working on a problem until it is resolved
3. We proactively monitor our industry to have an early warning of emerging issues
4. We can make tough decisions quickly
5. We are known for our ability to use knowledge in novel ways
6. We build relationships with others we might have to work with in a crisis
7. If key people were unavailable, there are always others who could fill their role
8. There are few barriers stopping us from working well with other organisations
9. Our organisation maintains sufficient resources to absorb unexpected change
10. We have clearly defined priorities for what is important during and after a crisis
11. We have a focus on being able to respond to the unexpected
12. Given our level of importance, I believe the way we plan for the unexpected is appropriate
13. We believe emergency plans must be practised and tested to be effective

Answers provided are tabulated and a resilience score is developed. The meaning of resilience scores are listed below:

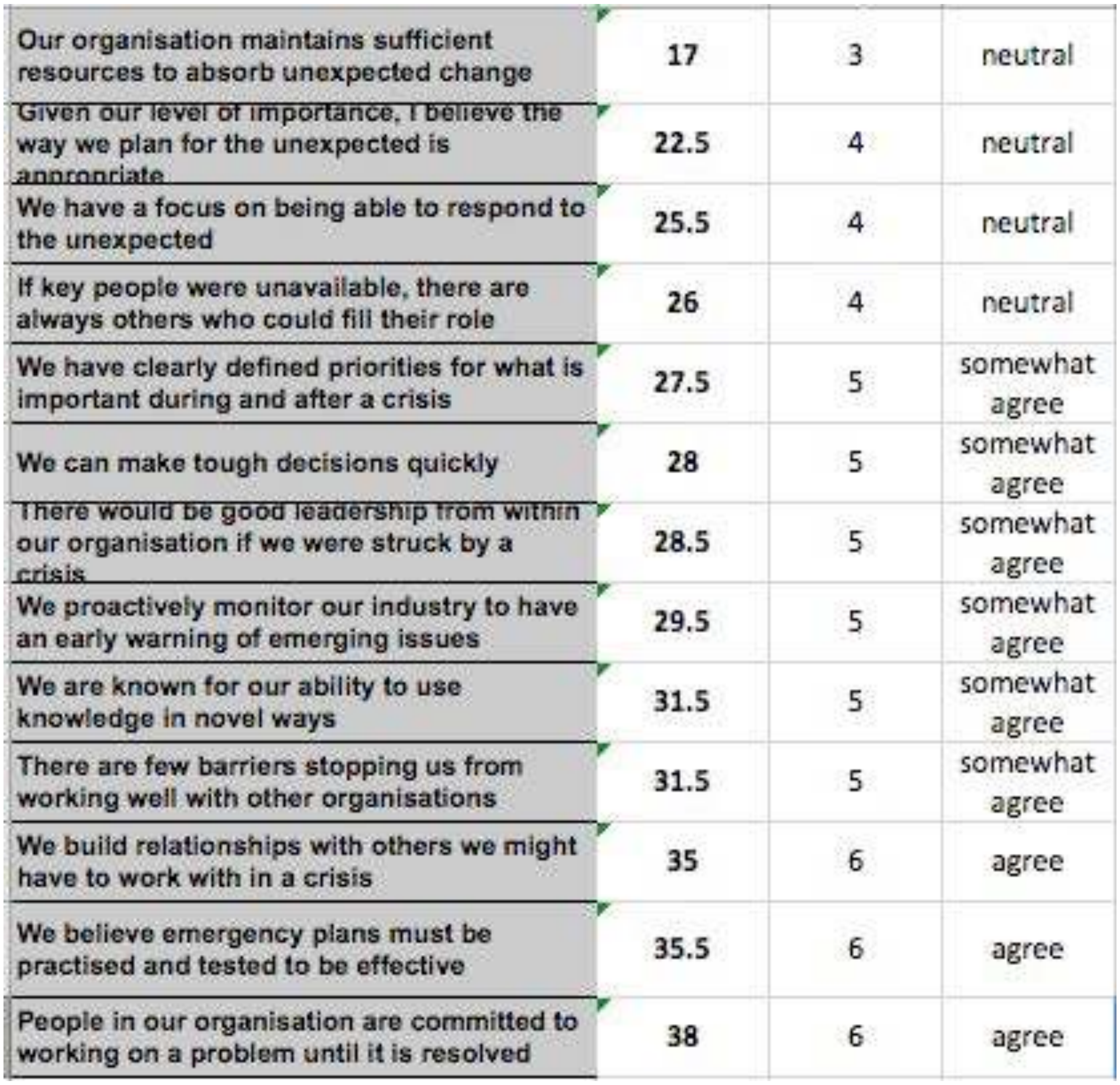
0 – 55: Low resilience:

56 – 67: Medium resilience:

68 – 91: High resilience

There was a total of five respondents for this survey, where one organization was ranked low, two were ranked medium and two were ranked high.

Indicators of resilience listed from low to high:



Our organisation maintains sufficient resources to absorb unexpected change	17	3	neutral
Given our level of importance, I believe the way we plan for the unexpected is appropriate	22.5	4	neutral
We have a focus on being able to respond to the unexpected	25.5	4	neutral
If key people were unavailable, there are always others who could fill their role	26	4	neutral
We have clearly defined priorities for what is important during and after a crisis	27.5	5	somewhat agree
We can make tough decisions quickly	28	5	somewhat agree
There would be good leadership from within our organisation if we were struck by a crisis	28.5	5	somewhat agree
We proactively monitor our industry to have an early warning of emerging issues	29.5	5	somewhat agree
We are known for our ability to use knowledge in novel ways	31.5	5	somewhat agree
There are few barriers stopping us from working well with other organisations	31.5	5	somewhat agree
We build relationships with others we might have to work with in a crisis	35	6	agree
We believe emergency plans must be practised and tested to be effective	35.5	6	agree
People in our organisation are committed to working on a problem until it is resolved	38	6	agree

Survey findings

Barriers to resilience (ranked neutral) / Weaknesses

- Lack of resources, planning, uncertainty about planning for the unexpected, backup staff identified

Strengths

- Good at building relationships, believe in good plans, good at working through a problem until resolved

- Problem with the survey — assumes they have plans, do plans… but they don’t actually do them.. But believe in them

- Average responses ranged from neutral to agree

Comments provided on survey (Raw data)

Comments on how the survey aligns with context:

The neutral answer to me also means 'I don't know'. Some aspects don't apply directly to me as I don't have my own dedicated staff (but some volunteers scattered around the world)

It applies partially to the kind of threats my organization faces but it sounds like it's more appropriate for companies and the business environment.

pretty well

The survey does align with most of the work that we do in our organization and in certain areas, we maynot be thinking as much as we should.

I think its vague. Was not sure how to respond on certain questions.

On general, all the questions are applied to Colnodo, but it is very important to recognize there are different kind of risk like economic risks, of human resources, in the develop of projects, etc. Some times the answer depends of the kind of risk which

Analysis

- Neutral was also “I don’t know”

- Difficult to apply to individuals

- Questions seem more targeted to business environment / companies

- Highlighted what they should be thinking about — educational / capacity building value

- Seemed vague, some questions difficult to answer

- Doesn’t accommodate for the different types of risks they face — felt the answer depended on the type of risk faced

Annex G. Interview / Focus Group Protocol Document

Evaluating Resilience

1. What does resilience mean to you?

Organizational Resilience

2. How would describe a resilient organization?

   <talking points>

   1. What factors e.g. (btwn 2-5) / description contribute to a resilient organization?
   2. What factors / how would you describe contribute to the **development** of a resilient organization?
   3. What factors hinder organizational resilience?

Resilience Assessment Tool

3. Do you consider your organization resilient? Please explain.
   1. Had you assessed resilience before using another tool?

4. How did the survey align with your perception of your organization's resilience?
   1. Did your perception change after the tool? If so, how?

5. How useful was the survey?

6. Have you considered any actions as a result of the survey? Explain.

Run through their resilience score and responses that stick out

1. Ask for justification, more elaboration (Survey questions below)
2. There would be good leadership from within our organisation if we were struck by a crisis
3. People in our organisation are committed to working on a problem until it is resolved
4. We proactively monitor our industry to have an early warning of emerging issues
5. We can make tough decisions quickly
6. We are known for our ability to use knowledge in novel ways
7. We build relationships with others we might have to work with in a crisis
8. If key people were unavailable, there are always others who could fill their role
9. There are few barriers stopping us from working well with other organisations
10. Our organisation maintains sufficient resources to absorb unexpected change
11. We have clearly defined priorities for what is important during and after a crisis
12. We have a focus on being able to respond to the unexpected
13. Given our level of importance, I believe the way we plan for the unexpected is appropriate
14. We believe emergency plans must be practised and tested to be effective

7. Describe the applicability of the Resilience Assessment Tool to your organization?
   1. Does anything need to be added? removed? changed?

Network Resilience

8. How would describe a resilient network?

   <talking points>

   1. What factors e.g. (btwn 2-5) / description contribute to a resilient network?

    2. What factors / how would you describe contribute to the **development** of a resilient network?
    3. What factors hinder organizational network?
2. Describe the applicability of the Resilience Assessment Tool to a network?
    1. Does anything need to be added? removed? changed?
    2.

Annex H. Resilience Assessment Tool Feedback

Partners had the following comments about Resilience Assessment tool:

1. There would be **good leadership** from within our organisation if we were struck by a crisis
    - Leaders need to be able to articulate ideas / vision / knowledge
    - Leaders need to turn implicit knowledge into explicit knowledge
    - Need to assess leader vs. staff perceptions
    - Need to find common timezones, common spheres of work (people working in a similar area)
        - Develop strengthen spheres and develop outwards to network —> develop smaller networks within the network
        - Opinion is smaller network is more resilient —> thought that resilience in larger networks come from smaller networks
2. People in our organisation are committed to working on a problem until it is **resolved**
3. We proactively **monitor** our industry to have an early warning of emerging issues
    - 3 - difficult to monitor in a country that is so regulated e.g. Tibet
    - 3 - Difficult to monitor inside tibet; human rights issues are priority and internet freedom censorship sometimes takes the back seat (bigger priorities)
    - Need a holistic picture of threats —> allows response to specific threats
    - Taking crises as fluid
4. We can make **tough decisions** quickly
    - 4 - decision making is difficult when people aren't together — some may be left out of decision making bc. Of time zones; need to discuss but not possible; need dynamics of discussion
    - 4 - difficult to make decisions with distributed nature
        - Distributed implies some people may not be part of the decision making
        - Time zones are a challenge
        - When physically together it's easier
    - Need to be more creative, make quicker decisions
5. We are known for our **ability to use knowledge** in novel ways
    - Process to learn from failures / good examples from others
6. We build **relationships** with others we might have to work with in a crisis
    - doesn't apply because working independently (for individual member)
    - Need to identify what the CSN role is to support one another in a crisis
7. If key people were unavailable, there are always **others who could fill their role**
    - 7 - normal situation has changed; challenging for different reasons
    - 7 - People need experience, beyond knowledge, to respond quicker

  - There are people that can step up, but not as well
8. There are few **barriers** stopping us from working well with other organisations **(collaboration)**
9. Our organisation maintains sufficient **resources** to absorb unexpected change
    - 9 - Growing very quickly makes it hard to adapt
    - 9 - Having a plan is one thing, but can't be top-down — must be from bottom up
    - 9 - when working from funding — difficult to allocate resources to backup when grant is just for the project — can't save for crisis / future use
10. We have clearly **defined priorities** for what is important during and after a crisis
    - Unexpected transition of organization — Unconscious shift from media to advocacy organization e.g. Global voices
    - 10 - Ensuring continuous support for community the org relies on — rapid response team
    - Technology is secondary consideration, behaviour of the people should be first
11. We have a **focus** on being able to respond to the unexpected
    - Not prepared for the unexpected
    - 13 - weren't facing it the unexpected
    - 11 - Security standards low because of org culture, lack of awareness of threats
12. Given our level of importance, I believe the way **we plan** for the unexpected is appropriate
    - 14 - No contingency plans in place
    - 14 - disagree
    - 13 - Written procedures — for finance, dev projects, etc., consumes time but believed to be useful for the organization
    - 12 - Insufficient resources to build resilience / security
    - 12 - No resources
13. We believe **emergency plans** must be **practised** and tested to be effective
    - 13 - Haven't done —> you don't think about it when you work in security
    - Having written / knowledge explicit helps organization continue w or w/o leaders

Annex I. CSN Security Protocol – Draft Framework

- **PREPAREDNESS**
- **At Work**
  - Checklists
    - Storage of Documents
    - Checklist of how to prepare at work (Grab and Go Kit)
    - Evacuation Checklist
    - Safe Research
    - Security Screenings
  - Instructions
    - Commuting to/from work / meeting
    - Guests / Visitors
  - SOPs (Normal)
    - Use of Security Equipment
    - Secure Communications
    - Coordination
    - Decision Making
    - Secure Data Storage
    - Roles & Responsibilities
- **At Home**
  - Checklist for Preparedness Kit
  - Evacuation Plan
  - Communications Plan
- **Travel**
  - Pre-Travel
    - Personal
      - Local / International
        - Identify Check-in times
        - At Home
          - Tips for the home while away
      - International
        - Checklist
          - Get Insurance
          - Check Travel Advisories
          - Checklist for Family / Workplace
            - FORM
          - Book Hotel
            - Floor 3-6, Back facing
          - Book travel to hotel
          - Medication

          - Check health status of country
          - Vaccinations
          - Check country regulations on drugs
        - Make a copy of important documents
        - Bring extra passport photos (visa)
        - Get Security Briefing
          - Embassy
        - Flight Booking
          - Safest right behind wings
        - Card w Directions to hotel in local language
        - Bring security equipment
          - CHECKLIST
        - Register with Government (If applicable)
          - ROCA
        - Configure VPN
        - Communication mechanism
          - If not secure to report
        - Border crossing prep
          - Identify message justifying travel — identify how clandestine you want to be
    - Country Specific Hazards
      - Dubai
      - Thailand
      - Mexico
      -
  - Organization
    - Security Briefing
      - Deleting all data
    - Store important documents
    - Store travel checklist
    - Identify list of country experts & likeminded embassies
- **IN COUNTRY**
  - Accommodation
    - Evacuation Route / Fire Escapes

  - Operations
    - Walking around
      - Pay attention to walking patterns
      - Be the “grey man”
    - What to carry / not carry
      - Mugger money

        - Computer
      - Cultural Sensitivity
        - Dress code —> what is culturally appropriate

      - Research
        - Vetting mechanisms for interviewees
        - Interview guidelines
          - Public place
          - Share description of who, where, when you're meeting, level of risk
          - Bring ID and emergency contacts
        - Dealing with the authorities

    - In Transit
      - Split up assets between passengers

    - **RESPONSE**
- General
  - Contact List (Network General)
    - Fan Out List
    - Org Specific
    - Canadian Specific
      - Travel.gc.ca
      - First Responders (Fire, Ambulance, Police, Poison, Psycho)
      - Psycho centre
      - 911
    - Include backup contacts
  - Activation Levels
    - Declaration of an Emergency
    - Level 0 - Normal —> Level 3 - Activation Descriptions
      - Network General Steps
      - Org Specific Steps
  - Communications
    - Ex. Media Lines
      - Org Specific Lines
  - Psychosocial
    - PTSD Diagnostic Checklist
    - PTSD Treatment suggestions
      - Org Specific Resources
  - Workplace
    - Alt Site Specifics
    - Evacuation
  - Situation Assessment
    - Checklist of info to collect

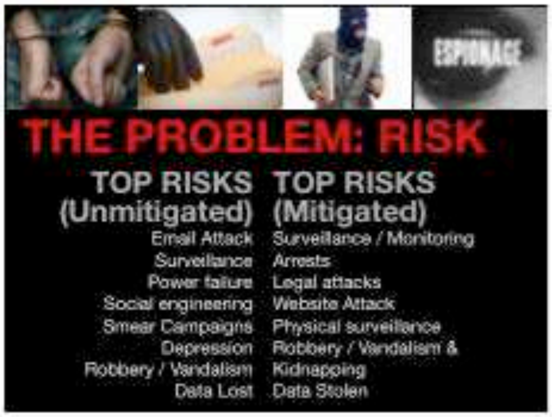
  - Coordination
    - Roles & Responsibilities
      - New Node
- SOPs (Crisis)
  - Digital Cyber
    - Website Attack
    - Compromise
      - Emergency File Destruction
      - Situation Assessment
  - Political / Legal
  - Psychosocial
    - Smear Campaigns / Social Engineering
  - Physical - Hardware / Data
    - Data Loss / Stolen
    - Legal Attack
    - Leaked Documents
  - Physical - Human
    - Arrest
    - Kidnapping
    - Terrorist Attack
    - Stalker
  - Natural
  - Organizational

- Templates
  - SOPs
  - Fan Out List
  - Contact List
  - Travel Info Form

Annex J. Crisis Simulation Deck

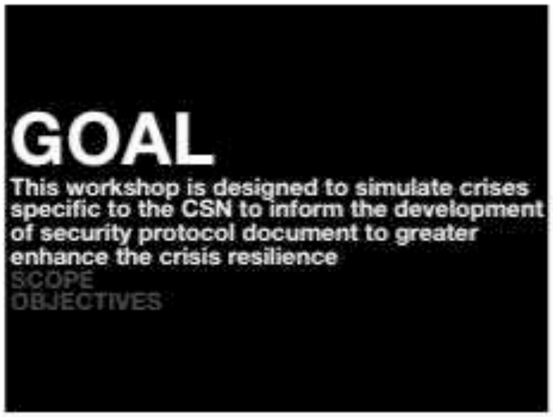
CYBER STEWARDS
WORKSHOP 3
Toronto, Canada | 04.01-04.03.2014

Session:
Security Exercise



THE PROBLEM: RISK

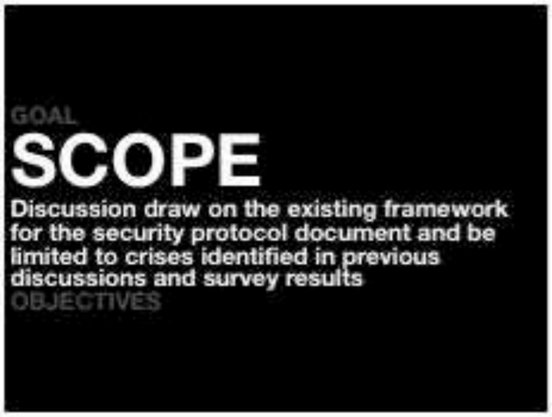
TOP RISKS (Unmitigated)	TOP RISKS (Mitigated)
Email Attack	Surveillance / Monitoring
Surveillance	Arrests
Power failure	Legal attacks
Social engineering	Website Attack
Smear Campaigns	Physical surveillance
Depression	Robbery / Vandalism &
Robbery / Vandalism	Kidnapping
Data Lost	Data Stolen



GOAL

This workshop is designed to simulate crises specific to the CSN to inform the development of security protocol document to greater enhance the crisis resilience

SCOPE
OBJECTIVES

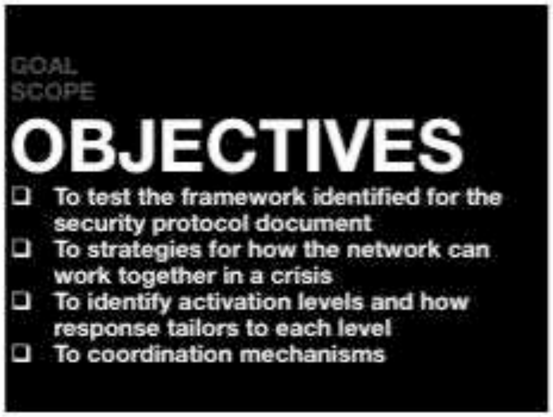


GOAL

SCOPE

Discussion draw on the existing framework for the security protocol document and be limited to crises identified in previous discussions and survey results

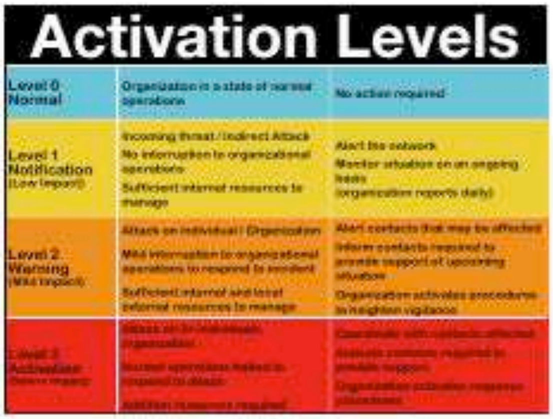
OBJECTIVES



GOAL
SCOPE

OBJECTIVES

❑ To test the framework identified for the security protocol document
❑ To strategies for how the network can work together in a crisis
❑ To identify activation levels and how response tailors to each level
❑ To coordination mechanisms

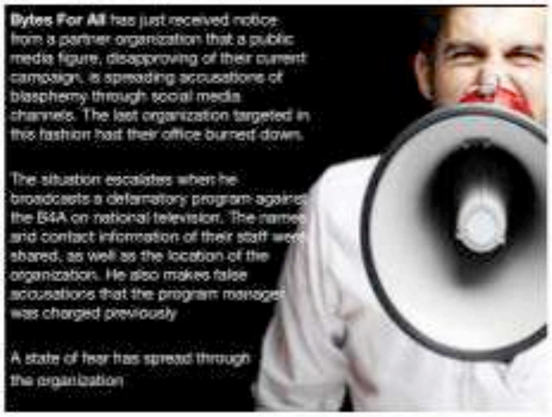


Activation Levels

Level 0 Normal	Organization in a state of normal operations	No action required
Level 1 Notification (Low Impact)	Incoming threat / Indirect Attack No interruption to organizational operations Sufficient internal resources to manage	Alert the network Monitor situation on an ongoing basis (organization reports daily)
Level 2 Warning (Mild impact)	Attack on individual / Organization Mild interruption to organizational operations to respond to incident Sufficient internal and local informal resources to manage	Alert contacts that may be affected Inform contacts required to provide support of upcoming situation Organization activates procedures to heighten vigilance
Level 3 Activation (Severe impact)	Attack on an individual / organization Normal operations halted to respond to attack Additional resources required	Coordinate with contacts affected Activate contacts required to provide support Organization activates response procedures

EXERCISE! EXERCISE! EXERCISE!

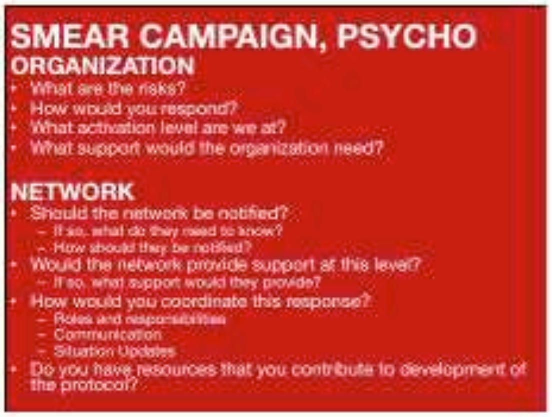
Attack of the Media Maniac



Bytes For All has just received notice from a partner organization that a public media figure, disapproving of their current campaign, is spreading accusations of blasphemy through social media channels. The last organization targeted in this fashion had their office burned down.

The situation escalates when he broadcasts a defamatory program against the B4A on national television. The names and contact information of their staff were shared, as well as the location of the organization. He also makes false accusations that the program manager was charged previously

A state of fear has spread through the organization



SMEAR CAMPAIGN, PSYCHO

ORGANIZATION

- What are the risks?
- How would you respond?
- What activation level are we at?
- What support would the organization need?

NETWORK

- Should the network be notified?
  - If so, what do they need to know?
  - How should they be notified?
- Would the network provide support at this level?
  - If so, what support would they provide?
- How would you coordinate this response?
  - Roles and responsibilities
  - Communication
  - Situation Updates
- Do you have resources that you contribute to development of the protocol?

I Need More Coffee...