UNDRR
UN Office for Disaster Risk Reduction

SENDAI FRAMEWORK
FOR DISASTER RISK REDUCTION 2015-2030

SUSTAINABLE DEVELOPMENT GOALS

BRIDGING CYBERSECURITY AND DISASTER RISK REDUCTION
WORKING PAPER

UNITED NATIONS OFFICE FOR DISASTER RISK REDUCTION (UNDRR)
REGIONAL OFFICE FOR EUROPE

Context and the Landscape

Of all the technological security risks facing contemporary society with potentially large-scale implications, the growing threat of cyber insecurity to societal resilience and economic security cannot be overstated let alone overlooked. This alongside the risk of other major man-made hazards such as infrastructure disruption, and natural hazards including those attributable to climate-related extremes which may result in na-tech scenarios.

Economic losses in the global economy associated with cyber-related incidents range between US$400 and 575bn annually (Ganin et al 2017). The exact cost of cyber-crime is difficult to measure, but it is clearly growing substantially. One estimate completed by the Center for Strategic and International Studies (CSIS) and McAfee in February 2019 estimated that it has now reached as much as $600 billion, or about 0.8 percent of global GDP (Center for Strategic and International Studies (CSIS) and McAfee).

In one of the most connected economies in the world (the UK), the Office for National Statistics concluded for the first time in 2016 that fraud and cyber-crime represented the most prevalent crime types in the country: 5.8 million incidents in 2015 / 2016, of which 3.8 million were fraud and 2.0 million were computer misuse incidents (Sky News, 2016). The potential effect of such an event were illustrated poignantly by the Wannacry global ransomware attack of May 2017. According to UK authorities, whilst it was a fairly unsophisticated attack, WannaCry affected 300,000 computers in 150 countries, and seriously impacted National Health Service (NHS): "over a third of England's NHS trusts were disrupted, with over 6,900 NHS appointments cancelled and some patients needing to travel farther for accident and emergency care".

Of course, malicious cyber-crime in the form of a targeted attack is not the only source of cyber risk; viruses, ageing equipment and infrastructure failure, poor governance, and weak contingency planning can similarly pose risks.

At the time of publishing this working paper, **the world is wrestling with, and reeling from the effects of the Coronavirus (COVID-19) on all areas of life. The cascading impacts of a successful hybrid attack against national power grids during a period of national and / or global emergency, such as COVID-19, could be unimaginable in terms of their reach.** This is especially so at a time when citizens are being asked or required to stay at home unless travel is essential with social and business contact being conducted virtually on a scale which was until recently unprecedented; manufacturers are retooling to produce urgently needed medical equipment; global supply / food chains are already under immense strain not experienced since the last World War; connectivity is critical for first responders as well as other essential workers; and many thousands of patients are fighting for their lives on ventilators.

UN Office for Disaster Risk Reduction (UNDRR)

Contributing Authors: Dr Katja Samuel, Global Security and Disaster Management Ltd and Dr Hugo Rosemont (ADS Group United Kingdom)

37 Bvd du Régent Brussels
1000, Belgium
www.unisdr.org
www.preventionweb.net
T: +32 (0)2 290 49 54

@UNDRR_Europe

Such risks are further compounded by the fact that many of the small and medium sized companies on which much of national disaster response now relies are likely to come with their own cyber security related vulnerabilities, not least in terms of weak internal systems and processes. Clearly, as many governments, institutions and individuals focus on survival, especially protecting lives and economies, this represents an especially vulnerable time in terms of cyber risk posed by malicious actors.

A cyber event targeted directly against or indirectly affecting critical national infrastructure, such as our health systems or power grids, would be catastrophic at a time when many are already struggling to cope. The reality of such as threat is illustrated by the destructive attack in December 2015 on three Ukrainian energy distribution companies which resulted in electricity outages for approximately 225,000 customers across the Ivano-Frankivsk region of Western Ukraine.

In addressing such risks, whether natural or man-made, most Governments, together with the multi-national institutions within and alongside which they operate, need to give major policy emphasis and substantial weight to the well-versed 'prevention is better than cure' approach. This preventative motto is a crucial element of resilience, an overarching goal of which is to prevent or at least mitigate potentially adverse impacts of identified risks, including in terms of any associated cascading effects.

Commonly, such risks are not approached in a fully integrated manner especially in terms of reducing potential disaster risk through comprehensive, joined up approaches.

Although it would seem that the full potential of the Sendai Framework is not currently being realised in relation to the prevention of man-made and technological risk, it offers important principles in this regard, with an overarching exhortation to key stakeholders to rethink and innovate existing approaches.

Cyber Risk as an Inherent Element of DRR and Resilience

There is a variance of views, including among States, as to whether cyber risk should be approached – in conceptual, institutional, policy and operational terms – as not only a security issue, but also as one of DRR, thereby forming an integral part of the Sendai Framework. **Currently, there is inconsistent practice among States regarding the extent to which cyber risk is reflected within their national DRR strategies.**

Such divergences in practice are not attributable to the provisions of the Sendai Framework which makes adequate provision for DRR within the context of man-made and technological risk which extends to cyber risk, including hybrid scenarios. Rather they seem to be due to a number of different factors ranging from diverging national priorities and capabilities; to a traditionally dominant focus on natural disasters which historically has resulted in significantly more quantifiable insurance losses compared with man-made or technological events; to traditional practices of approaching cyber risk from a largely security / law enforcement rather than risk mitigation perspective; to a sometimes imbalanced focus on the DRR benefits rather than the accompanying potential risks of technological innovation.

This disconnect is despite the fact that the language of the cyber security community is commonly framed in DRR terms - such as prevent, protect, detect and respond – including to protect critical national infrastructure.

In light of the earlier discussion regarding the potential risks posed by hybrid threats, this is deeply concerning since in order for national disaster plans and responses to be most effective to realise optimal resilience they need to be comprehensive and joined up, especially in terms of identifying and integrating all potential sources of threat, risk and vulnerability. If the fundamental risk analysis and planning assumptions are flawed through incomplete identification of potential sources of risk then everything else that follows could be significantly flawed too. This could result in reduced resilience with potentially (more) catastrophic effects, including the occurrence of associated cascading disasters which might otherwise have been prevented or at least mitigated against.

Such potential vulnerabilities are especially concerning during a time of national emergency, such as the COVID-19 pandemic, which is so dependent upon the full and effective functioning of the health infrastructure to save lives.

However, in terms of key risk prevention and resilience lessons learnt from previous hybrid attacks and cyber related incidents, it is encouraging to note where other progress is being made. Notably, one of the specific hybrid threat scenarios identified as part of UNDRR's collaboration with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is **the potential for a cyber-attack with cascading effects on health systems, including compromising patient care by affecting healthcare monitoring devices.**

Opportunities and Options

For States and their critical national infrastructures to realise maximum resilience – in terms of their adaptability and ability to bounce back from cyber related incidents – a rethinking of existing approaches will be necessary. In response to the issues of potential vulnerability and resilience gaps identified, a number of options and solutions are made.

INTEGRATE CYBER-RISK IN NATIONAL RISK ASSESSMENT

Consideration should be given to "the multi-hazard management of disaster risk in development at all levels as well as within and across all sectors" exhorted by the Sendai Framework, thinking especially here of **increased integration of cyber risk within national disaster assessments** and planning not least due to its hybrid threat nature to impact directly on critical national infrastructure. This will necessitate that governments consider whether to "adopt one single plan covering all possible threats, or rather envisage […. the] adopt [ion of] hazard / risk specific strategies" (UN Office for Counter-Terrorism).

What such an approach means in practice is that "strategic objectives and organizational structures are shaped in such a way as to take into account accidental, intentional and natural threats to [Critical Infrastructure] in a holistic manner. An all-hazards approach is often seen as a prerequisite to make the best use of limited available resources and avoid needless duplication. The underlying rationale is that the same risk management and collaborative processes as well as crisis response mechanisms can be broadly used to respond to all types of threats indistinctively". In turn, this means that threats / risks - including cyber related ones – are approached in a more integrated manner, including in relation to hybrid threat scenarios touching on both physical and digital spaces.

RISK-INFORMED STRATEGIES

The Sendai Framework calls for effective risk reduction strategies to be in place, both locally and nationally, and for investments to be risk-informed and better target resilience needs. As highlighted in the UNDRR guideline on the development of DRR strategies (UNDRR, 2019), strategies should be geared to respond to potential cascading effects which will involve a complex tapestry of more interconnected security threats. **A comprehensive and all-hazards approach to risk reduction should integrate technological risks, notably here cyber security, in the strategic planning and decision-making of disaster risk reduction actions and investments.**

Not incorporating cyber risk fully or even at all within national DRR strategies is likely to impact negatively upon national resilience to cyber-attacks, including in terms of their ability to prevent as well as recover from them most effectively.

INCREASE ACCOUNTABILITY

In addition to the associated resilience benefits of more integrated approaches, it is important for key stakeholders to fully understand the potential legal and ethical implications of failing to strengthen known gaps and vulnerabilities. Under the doctrine of due diligence (comprising three limbs: to protect the population; to prevent harm; and to ensure the availability of appropriate remedies should harm occur), those **governmental and quasi-governmental actors involved with the protection of critical national infrastructure especially are required to take all reasonable and appropriate measures to reduce reasonably foreseeable cyber risk related vulnerability.**

STRESS TEST CAPABILITY TO WITHSTAND HYBRID AND CASCADING RISK SCENARIOS

To better understand gaps in addressing cyber threats, **stress testing existing risk management capabilities would support greater understanding of current capacities and improvements that may be required, cognizant of the fact** that an event of great magnitude or multiple failures at the same time could exceed all capacity. Stress Testing current mechanisms would facilitate better comprehension and strengthen the ability of various sectors and services to ensure business continuity and reduce potential impact.

Cyber security risks can induce the vulnerability of any society: a stress to the smallest of vulnerable elements in a highly-interconnected network of services and systems – characteristic of highly developed countries – can lead to shocks on a systemic scale. For that UNDRR, with the engagement of Hybrid CoE, has developed a Stress Test tool which is increasingly being put to use by governments in identifying complex scenarios including cyber related threats.

Way ahead

UNDRR
UN Office for Disaster Risk Reduction

Society's dependency on the resilience of information and communications technologies (ICT), within what is being called the fourth industrial revolution, cannot be understated. As they increasingly underpin the operation of all critical national infrastructure and other essential services, and as technology advances rapidly and the barriers to entry for cyber criminality lowers, so we need to rethink their digital integrity.

The greater likelihood and potential impacts and cascading effects of a major cyber incident, the more attention must be given to realising the 'reasonable and appropriate' threshold. Failure to do so could result not only in catastrophic harm along the lines discussed in this paper, but also could result in civil tortious liability, as well as individual and corporate criminal prosecution such as for manslaughter. Though the language of 'black swan' is commonly used in the context of discussions regarding catastrophic risk, including cyber related, against critical national infrastructure, the fact that they have been identified and are being discussed at all is suggestive of the reasonable foreseeability of at least some of these scenarios.

There are some encouraging signs that hybrid threats are increasingly viewed as a priority issue, including the initiative led by UNDRR to develop a stress tool to assist States to better comprehend and strengthen their ability to reduce the risk of hybrid threats with their accompanying potential for cascading disasters. Such developments, however, do not yet represent global trends. This is particularly true in terms of better integrating traditionally separate security / law enforcement and disaster risk factors. Clearly, there is much work still to be done.

This paper sets out some key reflections and recommendations on challenges and opportunities associated with bridging cybersecurity and disaster risk reduction aimed at assisting organizations to become more resilient in a rapidly evolving threat and risk landscape. Insights shared here are expected to be of relevance and interest to partners locally, nationally and internationally. A primary intention of this paper is to accelerate implementation of SDGs, the Sendai Framework for Disaster Risk Reduction 2015-2030 and contribute towards the 2021 European Forum for Disaster Risk Reduction.

Further reading

- **Sendai Framework for Disaster Risk Reduction 2015-2030.**
  www.undrr.org/implementing-sendai-framework/what-sf
- **Stress Testing helps withstand hybrid and cascading risk scenarios.**
  www.undrr.org/news/new-tool-helps-withstand-hybrid-and-cascading-risk-scenarios
- **United Nations Global Assessment Report.**
  https://gar.undrr.org/
- **Words into Action guidelines: National disaster risk reduction strategy** www.undrr.org/publication/words-action-guidelines-developing-national-disaster-risk-reduction-strategies
- **Words into Action guidelines: National disaster risk assessment**
  www.undrr.org/publication/words-action-guidelines-national-disaster-risk-assessment