100 Days Later

v 1.7

Covid-19: Implications for Managing Terrorism and Asymmetric Threats

CHC GLOBAL

START
NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

100 Days Later

BACKGROUND

As part of our ongoing collaboration, the teams from START and CHC Global have held a series of managed discussions to consider the potential impacts of Covid-19 on terrorism and asymmetric threats.

We have considered the implications for governments, businesses and individual citizens, with a focus on how terrorism risks might be evolving. It is likely that the current uncertainty is having a range of impacts on threat actors, but it is too early to determine any absolute truths regarding changes to the global terrorism risk profile. However, it is possible to look more broadly at what this event can tell us about how organizations might orient to risks which sit in the higher frequency – higher impact (the "upper right") quadrant of the risk register – including some forms of terrorism.

Since the first reported case outside China on January 13th, our views have been informed by validated open-source reporting. Just over 100 days later, this document summarizes the record of those discussions.

OVERVIEW

We've identified three strategic imperatives:

1. **Honest Risk Assessment.** Organizations should revisit their all hazards threat and risk assessments in the context of lessons identified from Covid-19. This is not a 'Black Swan' event; many risk registers will have included some form of 'pandemic'. We would refer to this as more of a 'Grey Rhino' - a large and unmissable risk that organizations identified, but for a variety of reasons, did not fully address. Given this apparent "blind spot", we suggest that all risks in the "upper right quadrant" should be revisited and appropriate plans considered. It is false economy to provide "light touch" solutions to these risks simply because they are "challenging", or because the cost of pre-event mitigation seems prohibitive. Intelligent and innovative solutions should be sought.

2. **Event Agnostic Resilience**. Whilst we are focussed on terrorism threats, the current situation warrants an all hazards approach. With so many threats overlapping and exacerbating one another, it makes sense to consider effects and consequences that are agnostic to any one initial cause. Developing a strategic resilience is most likely to equip an organization, or nation state, with the flexibility to respond to the complexity of real-world events. As a pragmatic starting point however, planning for the most challenging threats and risks, such as terrorism, can have measurable benefits across a range of perils.

3. **Public - Private Partnerships.** Response to major crises, and especially population-centric emergencies, require effective coordination between the public and private sectors – including risk financing. Governments cannot control the virus. Instead, they must influence populations to behave in ways that reduce risk over a protracted timeline. Whilst this can be achieved with "on the fly" improvisation, it is much more effective if a well-practiced and functioning relationship is embedded before an event. This starts with adopting a shared response paradigm, such as an emergency response or public health model, and is furthered by developing effective systems for interoperability, including the sharing of potentially sensitive information.

RISK CONTEXT

The global crisis created by Covid-19 has generated profound uncertainty. It is entirely credible that the 2020 – 2021 winter will bring another wave of infection along with Seasonal Influenza and that any "return to normal" is contingent on either vaccine or effective therapeutics. Whilst there are encouraging noises on possibilities, authoritative commentators make the point that the quickest previous route to vaccine took nearly 5 years. There are also several examples where no fully effective prophylactic or responsive treatment has ever been developed.

This overwhelming uncertainty undermines confidence in institutions and their ability to influence behaviour. This virus doesn't respond to soundbites and top-down governmental fiats will hold the line only so long in free and open economies ravaged by unemployment. Before medical science is able to resolve the long-term issue, institutions and individuals will have to employ a variety of influences to encourage populations to establish robust coping mechanisms, whether preventative or responsive.

In the absence of clarity and certainty from legitimate leadership, extremist ideologues expressing absolute confidence in the violent empowerment they offer can be very attractive to those feeling victimized, struggling for limited resources, or looking for someone to blame for the crisis.

Prior to February 2020, we felt we were entering a period of significant change to terrorism and other asymmetric perils. Macro pressures such as political polarisation, climate change and the challenges posed by the 4th industrial revolution still have the potential to influence groups already on the journey from protest to direct action.

Considering these pressures now, it is possible that the direct impacts of Covid-19, any perceived government failings in managing the virus, and opportunistic malign influence operations, will act as an accelerant to mobilise the disenfranchised or the reactionary. While the virus will pose tactical challenges for violent extremists, this environment has exacerbated the enabling conditions that foster mobilization to violence. We are already seeing "the system" straining in some jurisdictions to keep civil unrest at bay.

At the geopolitical level, major sources of potential destabilisation are uncertain and appear more volatile. Whether we look at US-China relations, the Domestic US, the EU, pressures in Sub-Saharan Africa, or ongoing tensions in the Middle East, governments will be relatively hard-pressed to offer empowering futures for their citizens, while the grievances, conspiracies and narratives which underpin violent extremist ideologies are all likely to be reinforced.

The response to Covid-19 itself will continue to be a polarizing election issue in the US and elsewhere and has already compelled domestic terrorists to plot violent attacks. Opportunistic terrorists and malign foreign influence operations smell "blood in the water" and will try to capitalize on already strained government capacities.

IMPLICATIONS FOR GOVERNMENTS

Given strategic uncertainty, questions of government legitimacy in the face of compounding crises, and opportunistic extremist movements, what might this mean for global security risks?

During this time of perilous uncertainty, it is entirely possible, if not likely, that another macro event will occur and run concurrently. This could be in the form of a significant natural disaster, a "hot" geopolitical situation, or a major terrorist attack. Countries and organizations may not have the time to "ride this out" and should actively be focussing on increasing their resilience. In order to achieve this, there is a requirement for a realistic and honest revisiting of the all hazards risk registers. Resilience planning should take a "peril agnostic" approach, to ensure suitable flexibility in response and recovery plans. These plans will require more effective mechanisms to be created across the public / private sector.

Given the state of play today, this is an attenuated crisis that cannot be neutralized through a decisive, top-down action. Instead, the severity of the crisis, and the corresponding vulnerabilities to other compounding crises, are a function of how populations behave over time as the virus' fate waxes and wanes. Influence, rather than control, is therefore paramount. Governments must work with private sector institutions, local authorities and charismatic individuals to influence behaviour broadly, fostering general risk reduction, or to displace risk away from points of greater consequence and vulnerability.

There is an increased risk of strategic miscalculation, particularly as we enter the US Election cycle. Countries which have previously engaged in "implausibly deniable" actions, could find an unexpected kinetic response from a particularly stressed US or Allied government. This has obvious escalation risks. At a time when all political leaderships are under domestic pressure to show decisiveness and provide certainty, there is a very real risk that an erroneous tweet, a diplomatic affront, or a traditional act of sabre-rattling, may be seen as demanding of a response.

In terms of a potential terrorist attack, we should recognise the significant vulnerability of most OECD nations to any malicious act. Fewer crowded locations may reduce the frequency and severity of some low complexity attacks, such as those using a vehicle as a weapon, but the current context creates other vulnerabilities.

Medical facilities, grocery stores and critical infrastructure serve as attractive targets; the psychological and real-world implications of attacks on them could be significant and would reverberate loudly through the media and economy. The frictional pressures of remote working and absenteeism are degrading many responders, and homebound civilians are less likely to observe and report suspicious behaviours.

Businesses have fewer resources to serve as a safety net for their employees. Supply chains are vulnerable to disruption. There is already strong evidence that organized criminal groups are effectively exploiting the online environment to engage in ransomware attacks on hospitals and other fraudulent schemes, and there is little to indicate that law enforcement responses are being effective in the cyber domain.

IMPLICATIONS FOR BUSINESSES AND CITIZENS

Given the risk context and governmental challenges, we can expect businesses and citizens to experience prolonged uncertainty. One of the most pronounced impacts of Covid-19 has been the direct impact on household finances due to a drastic rise in unemployment and the decrease in worth of retirement holdings. This acute stressor has the potential to be one of the motivators of domestic, workplace or extremist violence.

Initial studies suggest that consumption of extremist propaganda has increased as individuals spend more time online. Terrorist movements across the ideological spectrum have used Covid-19-related arguments to recruit new members, retain existing adherents, amplify conspiracy theories, direct hate and violence at specific targets such as the Asian and Jewish populations, and to foment civil unrest and distrust in the government. Thought will need to be given to how effective interventions, with employees or loved ones flirting with extremist content online, can be managed during lockdown conditions, and as some "go back to normal" while others remain unemployed.

A current and practical concern for most citizens and businesses is how and when lockdown pressures will be eased. For the knowledge economy, this may take the form of embedding and systemising what has been up until now, an expedient response to the outbreak. It is entirely conceivable that many organizations will consider remote working as the new norm; abandoning large office environments and seeking a fully mobile and flexible work approach. This option will not be open to all enterprises, but the corresponding shift in population is expected to have an impact on malicious targeting. Furthermore, remote working may make existing personnel reliability and insider threat programs obsolete.

These new conditions are likely to motivate terrorists to review their viable courses of action. Along with increased effort in the cyber domain, we could see the return to larger, so-called 'spectacular' attacks, aimed at locations that retain a significant emotional meaning to a specific population, such as iconic structures. We may see increased focus on government targets as well, with the potential for collateral damage and non-damage business interruption to those in close proximity. Extremist movements may also double-down on the violent, premeditated forms of civil unrest that have played out at protests and counter-protests over the last several years.

The significant financial impacts on businesses have demonstrated that the insurance markets are not well placed to respond to, nor are they designed to deal with, systemic risks. In other classes of risk, where the financial impacts are expected to sit above the capital available to reinsurers, governments and markets have created Protection Gap Entities (PGEs). In the context of terrorism, the PGEs across the OECD and other economies are relatively mature and represented by the International Forum of Terrorism Reinsurance Programs (IFTRIP). The structure for some kind of "Pandemic Re" is being discussed across many economies, in part based on the successful "Public Private Partnership" approach to terrorism. This shouldn't encourage the perception that the insurance of terrorism is "under control". Relatively recent events have demonstrated that SMEs remain extremely vulnerable to events generating non-damage business interruption. More importantly, the entire business community remains exposed to the risk of a systemic malicious cyber event, the financial impacts of which could rapidly mirror those from Covid-19.

Like governments, businesses should revisit their all hazards risk assessments objectively and consider both the frequency and severity of those events which might previously have been considered "outliers". Many organizations are moving rapidly to capture the "lessons identified" from Covid-19, but resilience will only belong to those who implement "lessons learned."