5 SO WHAT FOR DEFENSE?

5 SO WHAT FOR DEFENSE?

In this age of deep uncertainty and exponential technological change nobody can 'go at it alone'. NDOs should think strategically about their portfolio of partners. As we stated in the Introduction, although the Dutch defense organization already has a quite broad cooperation portfolio, it also tends to be somewhat lopsided. Historic and current cooperation choices exhibit a preference for long-term, formalized, closed cooperation setups with mostly like-sized, like-minded, and likewise organizations. These traditional kinds of cooperation clearly remain important. At the same time, the realization emerges that NDOs can gain a lot by also exploring *other* forms of cooperation – with unfamiliar partners and in more open and more loosely coupled ways, facilitated by new technological developments. In the words of CDS General Tom Middendorp: "I think it's of vital importance that we come to realize that we are all actors in a defensive ecosystem...Take Google or Apple for example with their mobile 'app' stores. They provide a free and open platform, that all sorts of 'ecosystem partners' can hitch a ride on. Both 'planned' and 'unplanned', while in the meantime allowing Google and Apple to benefit from the ideas, creativity, capabilities and actions of others. I wonder whether that is something that our defense organizations might learn from."

We fully concur with the CDS. For NDOs, the importance of 'with whom?'-decisions will only to increase. It is our sincere belief that the ability of NDOs to cooperate with a wide range of different partners, including ones that may differ dramatically from the defense organization itself, should be expanded. Moreover, this expanded ability to cooperate should be considered a key 'capability'. Such a capability has to be mainstreamed throughout the entire organization and cannot just be relegated to any one part of the organization or to an overriding 'cooperation department'. Doing so represents a number of great challenges. But its potential benefits are also outsized: we can think of no single force multiplier, both in terms of 'sensors' or in terms of 'effectors', that comes even close to this capability.

Below, we list three broad policy recommendations for NDOs to take advantage of the rapidly expanding range of ecosystem partners and cooperation forms that can be explored and exploited. In the final section of this Chapter, we then look at the three cases elaborated in this report, and draw some lessons at the more detailed and practical level of those particular cases. At this point, it is only fair to add that the Dutch defense organization already has taken steps along the route proposed below. To that extent, the recommendations serve as an encouragement to further implement the vision of CDS Middendorp of a defense organization fully and consciously embedded in true defense and security ecosystems, able to both strengthen and draw strength from those ecosystems.

5.1 COOPERABILITY IS BECOMING THE KEY SOURCE OF COMPETITIVE ADVANTAGE

The Westphalian and industrial age mindset has accustomed our NDOs to think of themselves first and foremost as "prime defenders" of our national sovereignty, analogous to the "first responders" in homeland security. In the heyday of the industrial age, this thinking was quite unequivocal. Today, the ethos, mindset and capability choices of NDOs are still very much influenced by it. In this frame of mind, NDOs see it as their responsibility to be able to do as much as possible on their own. Cooperation represents a residual activity, that is called upon when the own resources prove to be insufficient (as often is the case for small to medium-sized NDOs).

After WW2, this primary defender assumption was mutualized much in the way that insurance policies work: within broader and, still in the spirit of the industrial age, formalized alliances. Just as in the case of insurance policies, the policy holder was covered by the collective; in this case through the mutual assistance clauses Article V of the Brussels Treaty, Article V of the Washington Treaty and Art 42.7 of the TEU. Equally, just as insurance companies are worried that policy holders will take advantage of the coverage that they enjoy by behaving irresponsibly ("moral hazard", the equivalent of which is "free-riding" within NATO), so too did NATO try to develop equivalents for things such as policy premiums and deductibles – e.g. through the various capability targets of the NATO Defense Planning Process. The relative discipline that insurance companies, and the re-insurance companies behind them, were able to instill in the average private insurance policy holder has, unfortunately, not fully taken root in the broader "defense risk market". What we have seen in that market has been an increasingly reluctant but in many ways still indispensable public re-insurer in the form of the US.

In the transition to a new information age, however, it seems likely that NDOs will have to graduate to a different frame of mind. They may want to position themselves more as custodians of a broader ecosystem of a variety of actors that all contribute in their own way to promoting security and/or countering insecurity. Clearly "security" has become a complex concept, linking internal and external threats, geopolitics and geo-economics, state and non-state actors; the boundaries between organized crime, terrorism, espionage, and armed conflict have faded; and hybrid threats lead to a continuum between war and peace. (Only) a diverse and resilient ecosystem approach may mobilize enough variety, agility and mass to deal with the challenges at hand. Pursuing and fostering cooperation then becomes not a residual activity, but a core competence at the heart of the defense and security effort. As in business ecosystems, modern information technology, both physical and social, can be used to facilitate and stimulate cooperation with ecosystem partners. This means that strategic "cooperability" – the ability to interface effectively with very diverse partners from the broader defense and security ecosystem – may become even more important than operational interoperability.[269]

5.2 MONITOR AND EXPERIMENT WITH NEW FORMS OF COOPERATION TECHNOLOGIES

The main implication we draw from this broader trend is that our NDOs would be well advised to closely monitor and experiment with new cooperation partners and cooperation forms. The cases presented here are early examples of the breadth and depth of the new cooperation space that NDOs can explore and exploit. It is hard to deny that they are quite different from what NDOs are accustomed to. NDOs have a long track record of "technology watch". Most of that effort goes into monitoring the physical technologies that the hard sciences keep developing. The social technologies that humans develop and use to create (also new forms of) value are, in our opinion, at least as important as the physical ones that many organizations invest so much time and energy in.

An important corollary of this is the need to perform operational experiments with possible innovative portfolio options – in this case with new forms of cooperation. This allows for a better assessment of the relative merits. NDOs must find ways to run relatively low-cost experiments that, when deemed successful, can be scaled up. The Concept Development & Experimentation (CD&E) paradigm that has been introduced in many NDOs lends itself well to this approach. Some of the caveats that we mentioned in our case studies – as well as the remedies against them that have emerged in these new forms of cooperation – may present some useful lessons that can be heeded in setting up and rolling out such experiments.

5.3 SEE COOPERATION AS A PORTFOLIO CHOICE

Cooperation in defense and security is often viewed as a policy or even a political choice. When NDOs think of partners they think primarily of other NDOs. A decision to enter into an alliance with such partners is seen as primarily a political one. Geographical propinquity; political, socio-economic, cultural, or ideological proximity; historical linkages and cooperative experiences; even the personal chemistry between key political and/or military leaders may be sufficient grounds to make a strategic cooperation choice. It is decidedly not our intention to downplay the importance of these political motivations, let alone the imperative that such choices should be made by politically legitimate leaders. Every single one of these motivations represents much deeper ligaments that still offer unique sources of orientation and/or navigation guidance. The many linkages we currently have continue to be of unique value and there is no real reason to assume that this value will diminish in the foreseeable future.

What we do argue, however, is that what is – and should remain – a political choice should increasingly be informed by a more pragmatic, dispassionate, rigorous, a-/pre-political analytical stage. Partnership choices are in essence a portfolio choice. It is not just a matter of whether we want to work together with country A or B or with organization X or Y. It is a sound risk and uncertainty mitigation strategy to diversify the portfolio of partners. Rather than putting all eggs in one basket, it is always preferable to diversify those eggs over a few baskets. The key analytical question then becomes how to determine which baskets to choose. In a period of exponential and epochal change, this portfolio choice requires more premeditation than ever before. We should not lose sight of the fact that our NDOs have de facto already made such portfolio choices. There are excellent reasons, for instance, for the NDO to prioritize bilateral cooperation with countries such as Belgium or Germany and to foster the transatlantic bond. But we submit that, as we look towards the future, there are valid reasons to augment the basket of government-to-government relationships with closer, maybe even organic, affiliations with companies such as Google, IBM, or Microsoft; and with at least mutual, if partly implicit,[270] understanding and alignment of efforts with a host of NGOs.

5.4 LESSONS FROM THE CASES

Open Innovation. Innovation is crucial in order to stay competitive in today's global marketplace. Increasingly this requires companies and organizations to look beyond their usual methods, suppliers, and partners and tap into the full innovative power of all agents of change present in the entire ecosystem. This also goes for NDOs, which can no longer solely rely on trusted partners to harness the accelerating pace of technological – in a broad sense – developments. The InnoCentive case has shown how innovation platforms can potentially be a cost-effective tool for broadening the solution space, engaging with smart people with whom the organization would otherwise have never interacted with in the first place.

The open nature of platforms such as InnoCentive poses the risk of knowledge outflow. This is a sensitive issue not only for NDOs, but also for many companies that do not want tailor-made solutions to become available to competitors. To mitigate this risk, organizations can switch between open and more closed forms of cooperation depending on the sensitivity of the issue. NASA developed such an internal open innovation platform in collaboration with InnoCentive. NASA@work allows NASA's challenge seekers to post challenges that would only be available to NASA employees across its ten field centers without the risk of knowledge leakage.

Perhaps one of the most important lessons from using open innovation is that it is indeed a practice that does not necessarily take place in a static form of open participation but instead frequently moves between open and closed forms of cooperation. In this way, companies and organizations in the field of defense and security are better able to control the knowledge flow, while still reaping the benefits of open participation as much as possible. With cost-effectiveness increasingly being the overriding adagio in the defense industry, platforms such as InnoCentive can be beneficial in the sense that that a much larger spectrum of possible solutions can be scanned, potentially at a lower cost than in the case of traditional R&D, and with acceptable risks to knowledge outflow.

Tapping the hacker community. The past decade has seen a veritable rise in the number of cyber-attacks perpetrated by individual hackers, or by hacker groups that operate as a larger community. These acts could form part of a systematic campaign to destabilize a country, explicitly or implicitly state-backed. NDOs that wish to guard themselves against cyber-attacks have employed white hat hackers to test defenses and go after possible cyber-attack perpetrators. Cooperation between NDOs and white hat hackers is not a new phenomenon. The novelty would lie in employing black hat hackers. One reason to employ black hats could be their superior skillset compared to white hats. Since black hats focus exclusively on security penetration they should therefore better placed for the development of offensive cyber capabilities than white hat hackers.

The fundamental problem in recruiting black hat hackers is trust and loyalty. Resorting to strategies of coercion or cooption will do little to change this situation, although black hats could be used for targeted assignments in exchange for clear benefits, such as a reduced prison sentence or charges dropped. There are numerous examples whereby the FBI has successfully forced online criminals to cooperate in this manner. However, for offensive cyber capabilities, the preferred way or working with black hats is through the application of "soft power". This means convincing hackers to voluntarily engage in activities the NDO would want them to do. There are reasons to believe that participants in the DDoS attacks on Estonia in 2007 and Georgia in 2008 were motivated by broader national interest, rather than by coercion or cooption. The problem, however, is that this particular way of working does not assure the desired capability at a particular moment in time, at a desired scale, and with a guarantee of success.

Training and employing a force of white hats is a relatively secure option and a process through which a NDO would be able to exercise a significant degree of control. However, when it comes to offensive capabilities, these white hat hackers often are less skilled than their black hat counterparts and risk being outgunned. Compensating for this skill gap by working with black hat hackers – however limited in scale and scope – is likely to remain a highly uneasy partnership in the foreseeable future.

There is another angle for taking a closer look at how hacker communities operate from a NDOs' perspective. The success of cyber-attacks performed by hacker groups critically depends on cooperation between numerous individuals who often do not know each other and have never met in person. Such cooperation in the blind typically only works well in a high trust environment, precisely the kind of element that the hacker community generally lacks. Since anonymity is a central part of the online environment, it is difficult to determine who you can trust. In expanding their cooperation portfolio, NDOs are also bound to enter some low trust environments NDOs will engage not only in long-standing, high-trust partnerships, but also in more ad hoc, informal, and implicit forms of cooperation with unfamiliar parties, and even with parties considered untrustworthy or outright hostile. Hacker communities have found various ways around this problem, including the use of intermediaries and using hacker forums with invite-only channels. It would be interesting to see whether these kind of mechanisms could also be fruitfully applied in other low-trust cooperation forms NDOs might need to embark on.

Online platforms for building situation awareness / understanding. If anything, the Ushahidi case shows that when the need is high, ingenuity can lead to surprising new forms of cooperation. Before the earthquake in Haiti, Ushahidi had not been used in a humanitarian relief context, but proved to be highly useful for several reasons: it was a means that was quick to mobilize and furthermore helped to mobilize various constituencies, from volunteers to humanitarian relief organizations (HROs) to government organizations; it provided an adaptable platform; it was cheap; and it helped parties on the ground to get access to large amounts of information processed by way of crowdsourcing that would otherwise not be available. Specifically, it helped HROs get a better picture of the disaster area in a fraction of the time it would have taken had this been done by on-the-ground surveyors and helped them to better coordinate and allocate their resources to those areas and people that were most in need.

Given the makeshift way this new form of cooperation came about, various shortcomings also emerged. First, while crowdsourcing is a great asset in itself, there is also the drawback that interpretation of data was left in the hands of non-professionals. Thus, the accuracy of the information that was eventually reported left something to be desired. Another point is that privacy issues emerged, specifically in that information that was collected could be accessed by US intelligence agencies. Third, coordination between the different actors and platforms remained an issue throughout, in particular given the informal nature of the Ushahidi platform. Subsequently, however, Ushahidi showed its adaptability by implementing various changes that responded to the perceived shortcomings.

In all, the Ushahidi case demonstrates that in view of the big data revolution and the way in which people are interconnected these days. NDOs cannot ignore these developments in planning and undertaking humanitarian relief and peace support of operations, and possibly also operations beyond those. The challenge will be finding a way to coordinate the various platforms and actors that will likely be involved so as to improve the quality of actionable information produced. At the same time, the informal and nimble nature of platforms such as Ushahidi also have a virtue in themselves, meaning that too much coordination could stifle its comparative advantages in terms of obtaining vital information in a timely manner.