The Hague Centre for Strategic Studies

BETTER TOGETHER

Towards a new cooperation portfolio for defense

The Hague Centre for Strategic Studies

SECURITY

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

This report is from the HCSS theme SECURITY. Our other themes are RESOURCES and GLOBAL TRENDS.

SECURITY

HCSS identifies and analyzes the developments that shape our security environment. We show the intricate and dynamic relations between political, military, economic, social, environmental, and technological drivers that shape policy space. Our strengths are a unique methodological base, deep domain knowledge and an extensive international network of partners.

HCSS assists in formulating and evaluating policy options on the basis of an integrated approach to security challenges and security solutions.

BETTER TOGETHER

The Hague Centre for Strategic Studies

ISBN/EAN: 978-94-92102-34-8

AUTHORS Sijbren de Jong, Willem Th. Oosterveld, Stephan De Spiegeleire, Frank Bekkers, Artur Usanov, Kamal Eldin Salah, Petra Vermeulen, and Dana Polácková

COLLABORATORS Scott Ward, Clarissa Skinner

Graphic Design Studio Maartje de Sonnaville, The Hague

The Hague Centre for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
HCSS.NL

BETTER TOGETHER

TOWARDS A NEW COOPERATION PORTFOLIO FOR DEFENSE

The Hague Centre for Strategic Studies

TABLE OF CONTENTS

EXECUTIVE SUMMARY **11**

1 INTRODUCTION: COOPERATION AND HOW IT TAKES SHAPE **19**
1.1 CURRENT COOPERATION CHOICES AND THE NEED TO ADAPT 20
1.2 TOWARDS DEFENSE PORTFOLIO THINKING 21
1.3 DIMENSIONS IN COOPERATION SPACE 23

2 CASE-STUDY 1 – OPEN INNOVATION **27**
2.1 WHAT IS OPEN INNOVATION 27
2.2 WHY OPEN INNOVATION? 29
2.3 FORMS OF COOPERATION 31
2.4 INNOCENTIVE 32
2.5 NEW FORMS OF OPEN(ISH) COOPERATION IN DEFENSE 40
2.6 APPLICABILITY FOR NDOs 49
2.7 PRACTICAL EXAMPLES 52

3 CASE-STUDY 2 – THE HACKER COMMUNITY **57**
3.1 WHITE AND BLACK HAT HACKERS 57
3.2 COOPERATION BETWEEN HACKERS 58
3.3 COOPERATION BETWEEN NDOs AND HACKERS 61
3.4 BENEFITS OF COOPERATION 65
3.5 RISKS AND CHALLENGES 66
3.6 MODELS OF COOPERATION 70
3.7 APPLICABILITY FOR NDOs 72
3.8 PRACTICAL EXAMPLES 74

4 CASE STUDY 3 – 'USHAHIDI, AN OPEN PLATFORM FOR SITUATION AWARENESS' 79
4.1 USHAHIDI HAITI PROJECT 80
4.2 BENEFITS OF USING USHAHIDI 85
4.3 DRAWBACKS OF USING USHAHIDI 88
4.4 IMPROVEMENTS 91
4.5 APPLICABILITY FOR NDOs 93
4.6 PRACTICAL EXAMPLES 96

5 SO WHAT FOR DEFENSE? 99
5.1 COOPERABILITY IS BECOMING THE KEY SOURCE OF COMPETITIVE ADVANTAGE 100
5.2 MONITOR AND EXPERIMENT WITH NEW FORMS OF COOPERATION TECHNOLOGIES 101
5.3 SEE COOPERATION AS A PORTFOLIO CHOICE 102
5.4 LESSONS FROM THE CASES 102

6 FINAL OBSERVATIONS 109

ANNEX A: A FIRST DRAFT TAXONOMY OF COOPERATION 115

BIBLIOGRAPHY 121

ENDNOTES 137

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

This report is about cooperation, the way it is changing, and what this means for our national defense organizations (NDOs). We all know that cooperation helps solve challenges or achieve desired outcomes. In complex problems, it might even be a condition *sine qua non*. The downside is that cooperation also induces transaction costs. But the cost of organizations working together has been drastically reduced. For many organizations operating in an increasingly connected and therefore more complex world, both the pressure and the opportunities to cooperate have drastically increased. This different calculus has given rise to much more open, smaller scale – to the extent that individuals next to organizations have become part of the equation – and vibrant forms of cooperation, in many instances rapidly displacing traditional forms of stove-piped and closed cooperation models. In the business world, driven by competition and the process of 'creative destruction', the innovative drive leads to successful new forms of cooperation. In this report, we will look at concepts and examples from the business world and explore whether successes and lessons learned in the private sector can also be applied to our national defense organisations (NDOs), even in operational processes for which the 'business logic' of commercial markets has limited applicability.

The calculus underpinning cooperation choices has changed, and now favors more open, smaller scale and vibrant forms of cooperation

NDOs face a turbulent environment and an uncertain future. In these times of geopolitical shifts and exponential technological change nobody can go it alone – certainly not the defense organization of a small to medium-sized country such as The Netherlands. The importance of '*with whom*' choices for NDOs is only likely to increase. HCSS suggests putting a rich portfolio of cooperation partners and forms at the heart of the

Cooperation is not a binary choice; it is a portfolio choice from within a broader 'space' of cooperation options

strategic planning process. NDO partnership choices are typically thought to belong to the realm of politics, decided upon based on political preferences. This report argues they should rather be seen as value-for-money choices. Decisions should be made on the basis of a pragmatic, pre-political, pre-bureaucratic analysis that considers the various cooperation options that are available and then designs a portfolio of cooperation partners and forms that will enable an NDO to navigate very different futures.

The Dutch defense organization already manages a broad portfolio of cooperation partners. Its portfolio consists first and foremost of other NDOs with whom it work closely together. But its current portfolio goes far beyond these military partners. It includes other government departments or agencies; NGOs; local communities in their home countries and abroad; defense and non-defense industry partners or suppliers; knowledge institutes, etc. But in other crucial dimensions the cooperation portfolio tends to be more lopsided. NDOs exhibit a (historic) 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. But this report set out to explore *other* forms of cooperation that NDOs have thus far not had much experience with - with unfamiliar partners and in more open and more loosely coupled ways, facilitated by new technological developments. More in the 'digital' than in the 'physical' sphere: in the information age, 'connect and being connected' is more and more a prerequisite for being able to achieve strategic effects in many different domains. It this new age, defense and security challenges once again have become very much part of society and societal processes at large. Defense and security ecosystems that try to cope with these challenges are emerging. In the words of the Commander of the Dutch Armed Forces General Tom Middendorp: "I think it's of vital importance that we come to realize that we are all actors in a defensive ecosystem… we also have to explore other parts of this ecosystem."

We observe the greatest dynamism in the other parts of the cooperation space than where NDOs typically sit.

This report is based on the empirical observation that the most dynamic and promising new forms of cooperation in our everyday lives favor openness and loose coupling, while focusing on information rather than on physical assets. Examples include phenomena such as Wikipedia, open source soft- and hardware development, crowdfunding, etc. Many of these seem to defy common cooperation sense: they take very different organizational forms than our current companies; they tend to be highly distributed and peer-to-peer with unique coordination mechanisms; and they

are developing radically new business models to sustain their activities. But while dramatically different in nature, they seem remarkably effective and efficient. In some areas they are outcompeting the titans of the late-industrial age such as Microsoft or IBM, who themselves are also moving in that direction.

How can NDOs can learn from these new forms of cooperation? In order to answer this question, HCSS has explored three cases: InnoCentive, an open marketplace for R&D solutions; hacker communities; and Ushahidi, an open platform for crisis informatics. In this report, we describe how these new forms of cooperation are initiated, how they are managed, and what their strengths and weaknesses are. Do these cases point to new golden opportunities for NDOs? Our findings are somewhat mixed. On the one hand, these forms of cooperation clearly benefit from surprisingly advantageous characteristics when compared to traditional forms of cooperation in terms of entry, cost, scaling, space, speed, adaptiveness, and effectiveness. On the other hand, our case studies also reveal a number of prickly challenges in areas such as cultural resistance to change, quality assurance, command and control, information management and ethics. The case studies also explain, however, how these new forms of cooperation have developed quite effective ways to overcome some of these challenges. We want to emphasize that these case studies are not just about InnoCentive, Anonymous, or Ushahidi, but rather about the new forms of cooperation that they embody. In a short period of time, all of the example cases have learned and internalized many useful lessons, leading to impressive improvements. We submit that in all of these cases, the benefits can still be significantly enhanced and the drawbacks further mitigated.

Our case studies reveal some of the strengths and the weaknesses of new forms of cooperation. HCSS remains overall optimistic on their potential

The most promising case appears to be open innovation, which is gaining significant traction in many areas of public and private activity. NDOs have no alternative but to leverage the outcomes of the fast and high-quality innovation cycles in the commercial (civilian) market. At the same time, NDOs strive to keep the exact specifications and even performance range of their core capabilities hidden (*"mil specs"*), with the aim to ensure that would-be opponents do not acquire the same possibilities and to make it harder for potential adversaries to develop appropriate counter-measures. The challenge for NDOs is to have system integration processes in place that harness (fast) open innovation at the component level in continuous performance improvement while retaining the structural integrity at the system / platform and system-of-systems level.

The report concludes with some general recommendations that are, by and large, supported by the case studies. We note 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.

The first recommendation is that NDOs should move further along the road towards full-spectrum cooperability. This capability to engage in a broad portfolio of cooperation partners and forms should be treated just like the many other capability choices NDOs invest in. Developing cutting-edge defense hardware (e.g., jet fighters, frigates or land vehicles) requires meticulous long term investment, planning and refinement; so too does competitive full-spectrum cooperability. In many ways this particular capability may even be more difficult to achieve. It cannot just be procured or dealt with in a centralized "cooperation department", but has to be mainstreamed throughout the entire organization. But while representing a number of daunting challenges, its potential benefits are also outsized: we can think of no single force multiplier that comes even close. We suspect that as NDOs evolve towards broader strategic balance-of-investment methods, the net contribution of this capability will become even more apparent.

Track the cooperation space and experiment with promising areas.

The second recommendation is that our NDOs should monitor the entire cooperation space more closely than they currently do. Most NDOs engage in various forms of technology watch. There is still a clear bias in these efforts towards physical technologies at the expense of social technologies of the kind that we describe in this report. Given the growing importance of the entire defense and security ecosystem, we submit that our NDOs should devote more attention to monitoring real-life trends and developments in the cooperation space (as we illustratively do in this report) in order to remain situationally aware of new promising developments in this space. At the same time we also suggest they should go beyond that and experiment with various new forms of cooperation technologies. Some of the concrete incarnations of these new forms that we describe in this report (players such as InnoCentive or Ushahidi) may even represent good candidates for such experimentation efforts.

Cooperation choices are political, but they should increasingly be informed by a constant and rigorous 'portfolio analysis'

Finally, we recommend that cooperation choices be seen as portfolio choices that require pragmatic, evidence-based analysis and that can be and constantly are recalibrated based on that analysis. These choices should be made politically. But those political choices should increasingly be informed by a more pragmatic, dispassionate, rigorous, a-/pre-political analytical stage. It is a sound risk and uncertainty mitigation strategy to diversify the portfolio of partners. The key *analytical* question then becomes how to determine which baskets to choose. In a time where we are faced with exponential and epochal change, this choice admittedly requires more thinking than has ever been the case before. Without prejudging the outcome of this debate, we would encourage NDOs would ask themselves which partners represent the highest future potential defense and security return on cooperation investment: country A or B or companies such as Google, IBM, or Microsoft.

In an ever more connected and complex world, designing a more diversified portfolio of cooperation partners and cooperation forms becomes a strategic imperative for national defense organizations.

The Westphalian and industrial age mindset has accustomed our NDOs to think of themselves as "prime defenders" of our national security. 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). In the transition to the new information age, however, NDOs 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. Only a diverse and resilient ecosystem can mobilize enough variety, agility, and mass to deal with the challenges at hand. Pursuing and fostering cooperation then is no longer merely a residual activity; it becomes a core competence at the heart of the defense and security effort. In an ever more connected and complex world, designing a more diversified portfolio of cooperation partners and cooperation forms becomes a strategic imperative for NDOs.

Throughout the ages, actors that succeeded more quickly than others in seizing the opportunities embedded in emerging new physical and social technologies derived enormous – economic, but also defense and security – advantages over relative laggards. In the last major transition from the pre-industrial to the industrial age, Europe found itself in the lead of this process.

Consider full-spectrum cooperability as a key NDO capability to be treated on par with fighters, frigates and tanks

Today, Europe is no longer the undisputed leader on the leading edge of the new technological revolutions. But HCSS still feels that when it comes to the defense domain, Europe – and especially the smaller European NDOs – may still stand a better chance than many others to discover the optimal social technologies that befit these revolutions. We see current trends, especially (but not exclusively) in The Netherlands, of starting to think of "defense" as a "defense and security ecosystem", of which new style NDOs may be the best suited custodians. This might be seen as the present-day equivalent of how armies and militias gradually morphed into NDOs during the industrial age.

NDOs can no longer go it alone. Not today and certainly not in the future. They will be better positioned to achieve the defense and security objectives that their societies expect from them when they pursue those together with others. Better **together**. But in order to do so, they will also have to explore new and better ways of cooperating with others. **Better** together. We can already discern glimpses of how to cooperate better in some of the case studies we presented in this report; as well as in some concrete initiatives within the Dutch defense organization. The challenge that remains for all of us is to improve our ways to apply those to defense.

1 INTRODUCTION: COOPERATION AND HOW IT TAKES SHAPE

1.1 CURRENT COOPERATION CHOICES AND THE NEED TO ADAPT 20
1.2 TOWARDS DEFENSE PORTFOLIO THINKING 21
1.3 DIMENSIONS IN COOPERATION SPACE 23

1 INTRODUCTION: COOPERATION AND HOW IT TAKES SHAPE

This report is about cooperation, the way it is changing in the information age, and what this means for our national defense organizations (NDOs). We all know that cooperation helps solve challenges or achieve desired outcomes. In complex problems, it might even be a condition *sine qua non*. The downside is that cooperation also induces transaction costs. To what degree organizations seek cooperation then becomes a cost-benefit issue. But here is the crux of the matter: the calculus underpinning cooperation choices is fundamentally changing, mainly due to the ongoing ICT-revolution. The cost of organizations working together has been drastically reduced. For many organizations operating in an increasingly connected and therefore more complex world, both the pressure and the opportunities to cooperate have drastically increased. This different calculus has given rise to much more open, smaller scale – to the extent that individuals next to organizations have become part of the equation – and vibrant forms of cooperation, in many instances rapidly displacing traditional forms of stove-piped and closed cooperation models.

Our focus is on cooperation in the defense and security domain. In the analysis below, however, we will take concepts and examples from the business world and explore whether successes and lessons learned in the private sector can also be applied to our NDOs, even in operational processes for which the 'business logic' of commercial markets has limited applicability. Driven by competition and the process of 'creative destruction', the innovative drive in finding new forms of cooperation is conquering new heights every year. Some of these seem remarkably efficient. Let us take a look at an example that we are all familiar with. Encyclopedias used to be the result of one particular type of cooperation in which a for-profit commercial company paid a number of contributors a fee to write high-quality entries in a printed multi-volume edition that was sold (at a relatively high price) to as wide a group of paying customers as possible. Encyclopedia Britannica, for instance, employed a relatively small number of in-house editors who contracted some 4500 contributors – typically eminent credentialed

experts in their fields who were paid for their contributions – to write their entries. Customers paid thousands of dollars to acquire these lavishly produced tomes that they kept in their libraries for longer periods of time. Wikipedia, on the other hand, is the result of the mass cooperation of millions[1] of unpaid volunteer contributors who operate based on self-imposed but fairly strict rules under a non-profit organization. It is constantly updated and freely accessible to anybody with internet access. One of the fascinating aspects of this cooperation is how multiple editors cooperate (and fight[2]) transparently (on the talkpage) on individual entries to produce high-quality entries. Many of us have come to rely on them.

This report has the following structure. This Chapter sets the scene by placing cooperation options and choices in a strategic context, and by describing in general terms the new strategic possibilities for cooperation strategies made possible by the ICT revolution. Chapter 2 through 4 turn our attention to three concrete cases of non-traditional cooperation forms that we consider to be of great promise for NDOs: 'open innovation', 'tapping into the hacker community', and 'Ushahidi, an open platform for situation awareness'. Chapter 5 lists the main recommendations we have drawn from this research effort for the ways in which NDOs might be able to widen their cooperation portfolios. Chapter 6 closes of with some final thoughts on the matter.

1.1 Current Cooperation choices and the need to adapt

The Dutch defense organization already has a fairly broad set of cooperation forms and cooperation partners. First and foremost, this set involves close, highly formalized and long-standing relationships with other NDOs of, often like-minded, allies within NATO or the EU. These relationships represent strategic choices, in which serious (political, financial, diplomatic, etc.) investments are made. Other relationship options can be more ad hoc, as in the case of the countries alongside which The Netherlands might find itself in various operations around the world. One could call these, to use the military levels of war (or echelon) analogy, 'operational' alliance choices instead of strategic ones – but they too represent a strategic choice at any given moment in time. However, the Dutch and other NDOs cooperate with far more than only with their military partners: with other government departments or agencies at home and increasingly abroad; with NGOs; with local communities in their home countries or abroad; with defense industry partners or suppliers; with knowledge institutes, etc.

But while their portfolio of partners is broad, it also tends to be somewhat lopsided. The recent joint Clingendael and HCSS report *Internationale Materieelsamenwerking* (International Materiel Cooperation) contains two tables describing existing and

potential international cooperation projects in which the Dutch defense organization participates.[3] These tables clearly 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. But this report set out to explore *other* forms of cooperation that NDOs have thus far not had much experience with – with unfamiliar partners and in more open and more loosely coupled ways, facilitated by new technological developments. In the information age, 'connect and being connected' is more and more a prerequisite for being able to achieve strategic effects in many different domains. It this new age, defense and security challenges once again have become very much part of society and societal processes at large. Defense and security ecosystems that try to cope with these challenges are emerging. Consider the words of the Commander of the Dutch Armed Forces General Tom Middendorp from his opening speech at the 2015 Future Force Conference.

From the opening speech of CDS General Tom Middendorp at the 2015 Future Force Conference

"I think it's of vital importance that we come to realize that we are all actors in a defensive ecosystem. A system that constantly reshapes itself... Parts of this ecosystem can be – and have to be – actively arranged and managed in conventional structures… However, as the custodians of our societies' security, we also have to explore other parts of this 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."

Outside of the defense world, a number of actors have stumbled onto new forms of cooperation that – at least in some areas – seem remarkably successful. Are there any lessons in this for NDOs and successes to be replicated? Can and should the current partnership portfolio of our NDOs become more diversified to leverage all the possible cooperation options that are out there?

1.2 Towards Defense PORTFOLIO thinking

Our NDOs are confronting a turbulent environment. Fundamental changes seem to emerge with increasing speed, vehemence, and impact. There is a growing recognition that the resulting new risks and opportunities require not just new strategies but also

a new approach to strategy itself. Most of us have become accustomed to defining strategy *purposefully* by identifying a strategic goal and then pursuing it. Increasingly, a number of fields are also emphasizing the need for a more *adaptive* and/or *experiential* approaches to strategy. Instead of (or: alongside) defining an end goal and then sticking to it, prudent planning recommends a more permanent orientation effort, whereby planning assumptions are constantly challenged and – wherever necessary – adjusted based on the changes that are occurring or anticipated in the environment. Building upon this permanent monitoring process, the concept of *navigation* should be adopted, in which actors (can) constantly adjust their course to keep their ship afloat in turbulent waters and keep heading in the right direction. Over the past couple of years, the Dutch defense organization has put emphasis on the strategic function Anticipation, which underlines the importance of a permanent orientation and navigation processes.

In recent years, HCSS has emphasized the need for an additional analytical element that allows actors to straddle the gap between orientation and navigation. We have called that strategic element "strategic portfolio design". Portfolio thinking is widely recognized as one of the robust stratagems for hedging risk and uncertainty.[4] Financial experts, for instance, have elevated portfolio thinking to the standard approach to risk and uncertainty. But this fundamental and widely acknowledged stratagem for dealing with risk and uncertainty in investment choices could – and we suggest: should – also be applied to strategy itself. HCSS proposes thinking of strategy in terms of a broader 'strategy space': a multi-dimensional space with many plausible and desirable strategies that could be pursued. The main intuition here is to put a rich strategic portfolio at the heart of the strategic planning process and not a singular strategic choice.

Currently, NDO planners allocated to the planning of our capability portfolio are mainly focused on long-term acquisition of materiel. In our own view, three main 'forward'[5] defense planning questions are crucially important for any NDO: *what* can we do (policy options), *with what* (capability options) and *with whom* (ecosystem partner options). We regard all of these portfolio choices and the analysis behind the choices as being equally important. And yet right now, it is mainly the second question (with what?) that is receiving – albeit in our view often too limited[6] – attention through the defense acquisition process. The first (what?) and third (with whom?) questions are typically dismissed as ones that defense planners should not concern themselves with but that should be left to the political side of the house. We submit that they are not of a different (political) nature, but do require equal prior (pre-political, pre-ideological, etc.) analysis that is as dispassionate, rigorous, and transparent as the

analyses that should go into acquisition choices. Any such portfolio analysis, when properly done, is highly unlikely to yield unique answers. Instead, it is likely to highlight some key strategic trade-offs that (politically legitimate) decision-makers will have – and, we would hope, want – to be informed about when deliberating and finalizing their decisions. In previous and ongoing work, HCSS has and is already experimenting with a portfolio of policy options.[7] In this paper, we focus on the portfolio choices NDOs can make with respect to the 'with whom' question.

1.3 dimensions in cooperation space

What do we actually know about cooperation and the different forms it can take? Cooperation is an important topic of inquiry in many different academic disciplines. Biological lifeforms cooperate. Economic agents cooperate. Political movements and parties cooperate. States cooperate. Defense organizations cooperate. It is therefore quite surprising that we do not have a working classification scheme for the many different types of cooperation that exist in and across all of these different disciplines. The labels that are given to the various elements of cooperation differ from discipline to discipline. But in all of them we find back the entities that cooperate (who?), the purpose of their cooperation (why?), the nature of their cooperation (what?), the interfaces between them (how/through what?), and the broader system within which they cooperate (where?).

In preparing for this report, HCSS has started building a more general taxonomy of cooperation. This initial effort, contained in Annex A, is far from definitive – if such a condition exists at all for such a complex phenomenon as 'cooperation'. The main idea behind this try-out was to demonstrate that cooperation is indeed multi-faceted and is best thought of as a multi-dimensional option space rather than as a binary choice. To make this abstract idea of a 'cooperation space' somewhat more tangible, we have selected three key dimensions from that multi-dimensional space to further elaborate here, based on two considerations. One, they point to areas that appear new in the sense that NDOs are currently not investing much in this part of the cooperation space. And two, these new forms of cooperation are already successful outside of the defense and security realm and might be promising within that realm as well. In the Chapters 2 through 4 we will explore these new and promising areas in more detail through three case studies.

The first dimension differentiates between cooperation that deals with physical things and/or interactions and cooperation based on digital information exchange and sharing. The digital age is starting to enable radically different cooperation opportunities. In the

past decade, cooperation in the digital sphere has seen a lot more change than cooperation in the physical sphere. Examples of such forms of cooperation are Linux open source software, Wikipedia, purely digital cooperation between a client and her bank through online bank accounts, or github, where people build online software together.[8] Additionally, the digital and physical spheres are increasingly converging. Examples of such converging are 3D Manufacturing and the growing role that Computer Aided Design (CAD) is playing in the physical world.[9]

A second dimension is whether cooperation is tightly or loosely structured. Researcher Karl Weick developed the concepts of tight and loose coupling to describe organizational structures in educational institutions, but the same concept can be applied to businesses and governments. According to Weick, a tightly coupled organization has a set of mutually understood rules enforced by an inspection and feedback system, while in a loosely coupled organization, these are not in effect.[10] This means that in loose form of cooperation, there is less interdependency and entirely different forms of coordination and information flow. An example of a loose form of cooperation is the hacker community, where each hacker is an individual, even though certain hackers might cooperate in an attack. In a tight form of cooperation, however, there is much more interdependency, coordination, and information flow. An example of a tight form of cooperation would be the contracts the Dutch Defense organization has with other Defense organizations, or with companies such as Thales or TNO.[11] In these modes of cooperation, fixed contracts are set up with regular coordination and information flows.

The third dimension is the difference between open and closed innovation. In closed innovation, each company works on a service or product separately, keeping the manufacturing process secret (e.g. closed) to outside parties or companies. In open innovation, the manufacturing process is opened up so that people and organizations from outside the company can join in. An example of open innovation is General Electric's 3D printing contest. When General Electric found that it lacked knowledge to 3D print a light-weight jet-engine-bracket, the company organized a contest inviting people to engineer one for them. This became a huge success, after which the company started more initiatives.[12]

2 CASE-STUDY 1 – OPEN INNOVATION

2.1 WHAT IS OPEN INNOVATION 27
2.2 WHY OPEN INNOVATION? 29
2.3 FORMS OF COOPERATION 31
2.4 INNOCENTIVE 32
2.5 NEW FORMS OF OPEN(ISH) COOPERATION IN DEFENSE 40
2.6 APPLICABILITY FOR NDOs 49
2.7 PRACTICAL EXAMPLES 52

2 CASE-STUDY 1 – OPEN INNOVATION

In this and the next two Chapters we explore new and promising areas for cooperation in the defense and security domain in more detail through three case studies. In these case studies we explain how a few non-defense and security actors are taking advantage of new forms of cooperation to pursue their objective(s); describe to what extent our NDOs are already investing in these areas; and explore the advantages and disadvantages for NDOs to invest more in these areas.

These case studies constitute examples that might be helpful in systematic thinking about various models of cooperation for the type of large organizations that NDOs constitute. The examples were selected based primarily on their relevance for NDOs and the availability of information. Another factor was the genuine novelty of these forms of collaboration that did not exist until widespread adoption of the internet. NDOs can borrow some successful innovation practices from private companies and learn important lessons with regard to challenges and barriers in implementing open innovation.

2.1 WHAT IS OPEN INNOVATION

Despite the fact that there is no common definition of "innovation", it can generically be described as the process of creating value through idea development. In one of the earlier definitions, innovation was defined as "the generation, acceptance and implementation of new ideas, processes, products or services."[13] Baragheh et al. (2009) have pointed out that the definition of innovation has until now remained a discipline-specific process.[14]

Whatever its precise definition, innovation is crucial in today's quickly changing world. In order to stay competitive in the global marketplace, companies have to constantly develop better products, services, business models, or processes. Previously, companies relied predominantly on their internal resources, such as research and

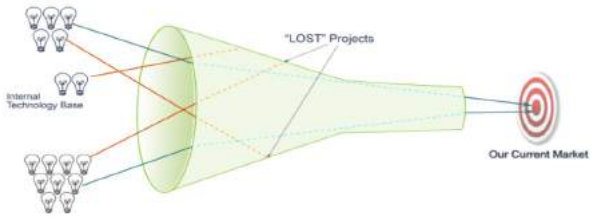

FIGURE 1: CLOSED INNOVATION. SOURCE: EIDON LAB, 2011.

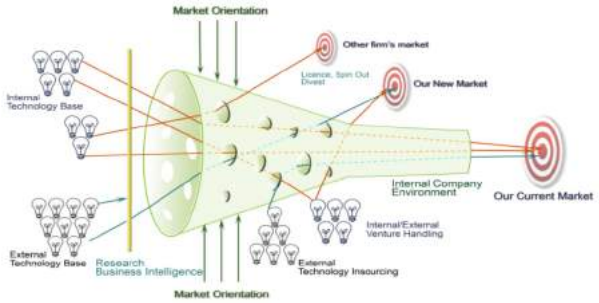

FIGURE 2: OPEN INNOVATION. SOURCE: EIDON LAB, 2011.

development (R&D) facilities and staff, to develop new ideas into viable products and services ("closed innovation", see Figure 1).[15] However, in the last two decades many companies have been actively pursuing increased involvement of external parties in their innovation processes. The concept that firms should look "outwards" for ideas and knowledge from a broad range of outside sources instead of just "inwards" is known as "open innovation". The term open innovation was introduced and popularized by Henry Chesbrough, professor at the University of California, in particular in his book *Open Innovation: The New Imperative for Creating and Profiting from Technology* (2003).

The idea behind open innovation is not particularly new. The academic science has always been an example of open (albeit traditionally fairly slow) innovation: collaboration between various researchers has been a norm and the results of research have been broadly shared via seminars, academic journals, the internet, etc. In the corporate world, customers, competitors, and suppliers have been an important but, most often, informal source of new ideas for a long time. R&D collaboration between the private sector and universities and applied science institutes (such as the

Netherlands Organisation for Applied Scientific Research, TNO) has been growing since the end of World War Two (WW2). However, most companies still see innovation to a great extent as a proprietary, closely guarded process, collaborating only with a small number of carefully selected organizations.

In contrast, open innovation relies on collaboration with a much larger pool of actors than was previously the case, including small companies, ad hoc informal groups, or individuals (see Figure 2 and Table 1).[16] It often involves ceding important decisions about the content of products to these networks of external participants. For this reason, some authors see open innovation as "democratized" innovation.[17]

"CLOSED" INNOVATION VIEWPOINT	"OPEN" INNOVATION VIEWPOINT
Nobody can know what we are innovating	Nobody can know the confidential ideas that we are working on
Spending more on internal R&D will improve our market position and help us to grow	"Smart" innovators engage with the global innovation community and reap the highest returns
First-to-patent = highest profit	First-to-market = highest profit
We need more R&D staff to close our knowledge gaps	We need our R&D staff focused on our core competencies, allowing outside solution providers to provide the rest

TABLE1: CLOSED VS. OPEN INNOVATION. SOURCE: EIDON LAB, 2011.[18]

Open innovation is a relatively new term and its exact characteristics are still debated. It may, at least, partially overlap with other similar terms such as user innovation, mass innovation, distributed innovation, crowdsourcing, etc. There are no clear boundaries between these terms.

2.2 WHY OPEN INNOVATION?

"No matter who you are, most of the smartest people work for someone else" – this phrase is attributed to Bill Joy, co-founder of Sun Microsystems, and it became known as Joy's law in the high-tech industry.[19] It describes the basic fact that for all organizations, relevant information and expertise residing outside an organization's boundaries significantly exceed those inside the organization.

Private companies have always been interested in accessing external sources of knowledge by using various forms of cooperation such as alliances, joint ventures, licensing agreements, and other means. Typically, these forms of cooperation focused on a careful selection of the limited number of organizations (or experts) that would

have the necessary resources or expertise, and included extensive negotiations between the parties involved and detailed legal contracts. The development of information and communication technology in recent decades and, in particular, the widespread availability of the internet have drastically reduced the costs of communication and created opportunities for radically disruptive forms of collaborative knowledge production. For instance, people with interesting ideas residing outside professional networks can now easily share them through blogs and other simple web tools. Wiki-style web sites, cloud-based platforms, social networks and similar tools enable large numbers of participants located in various parts of the world to work simultaneously on the same subject. The decline of long-term (for life) employment and the growing mobility of labor, in particular of highly-educated people, was another factor contributing to a wider distribution of knowledge.[20]

Technological and societal changes made open innovation possible and facilitated its adoption. But large organizations, especially business firms, have to see significant practical benefits in order to use this radically different approach to innovation. The potential benefits are numerous and might differ depending on a particular form of collaboration. In general, the major advantages of open innovation can be listed as follows:

- It provides an opportunity to access new sources of ideas and expertise. It stimulates the reuse of knowledge developed (and paid for) elsewhere, in what is called "knowledge circulation" within and across between different knowledge and application areas.[21]
- It might increase the speed with which an innovation track can be initiated and completed.
- It offers higher flexibility and responsiveness. Drawing on a much large source of potential collaborators, both quantitative (more experts) and qualitative (different experts) scaling can be achieved on a case-by-case basis.
- It might be less expensive. Outsiders might be cheaper than the full cost of insiders – similar to the cost benefits of outsourcing. Furthermore, payment might be contingent on meeting a set of requirements.
- It might increase the quality of a product. Involving a large number of people at much earlier stages in its development helps to remove errors and improve weak points, e.g. open source software, beta testing of software by companies such as Microsoft, crowdfunding, etc.).
- By involving users in its development, a product can be better tailored to users' need and requirements.

2.3 FORMS OF COOPERATION

In order to understand open innovation better, it is helpful to use a framework to organize various forms of collaboration taking place in this area. One framework that is simple and practical is provided by Pisano and Verganti (2008).[22] It lists four collaboration modes based on two parameters: the type of governance – hierarchical or flat (who makes decisions), and participation openness – whether anyone can participate or if there is a selection mechanism (see Table 2).

	INNOVATION MALL	**INNOVATION COMMUNITY**	Participation
	A place where a company can post a problem, anyone can propose a solution, and the company chooses the solution it likes the best	A network where anybody can post problems, offer solutions, and decide which solutions to use	Open
	ELITE CIRCLE	**CONSORTIUM**	
	A select group of participants chosen by a company that also defines the problem and picks the solution	A private group of participants that jointly select problems, decides how to conduct work, and choose solutions	Closed
Governance	Hierarchical	Flat	

TABLE 2: FOUR COLLABORATION MODELS. SOURCE: PISANO AND VERGANTI, 2008.[23]

Traditional forms of cooperation in the private sector in the science and technology field have used the closed mode of cooperation. Companies would carefully select potential partners based on a variety of factors: possession of a particular technology or capability, strategic fit, preemption of competition, and other factors. Most often, cooperation was also characterized by the hierarchical type of governance. One partner (such as a system integrator, e.g. Boeing in aircraft development) would be in charge and take key decisions.

The opposite of this traditional mode of cooperation are communities with open participation and flat governance. The most well-known examples of such a mode of cooperation are loose communities of programmers working on the development and improvement of open source software (OSS) such as Linux, Apache, Mozilla, and others. Between these two extremes there are two mixed models combining flat governance with closed participation ("Consortium" mode) and hierarchical governance with open participation ("Innovation Mall" mode). Examples of the former are consortiums that are often created for the promotion of a particular standard or technology (such as The DVD Forum, the Wi-Fi Alliance, or the Grand Alliance for the HDTV standard). The "Innovation Mall" mode is probably the most popular among companies engaging in open innovation and we consider a few examples in detail below.

Before considering specific examples we should note the important role that web-based tools play in enabling and facilitating open innovation involving a large number of participants that are spread out geographically. They take many different forms and are often called "open innovation platforms". Stoetzel et al.[24] classify open innovation platforms into four main clusters using two dimensions: platform purpose and platform operator (see Table 3).

PLATFORM PURPOSE				
	Understand Customers	Dell Ideastorm	Getsatisfaction	Identify customers ideas and needs
		Starbucks Idea	Suggestionbox	Customers can discuss and vote for ideas
		Ideas.nagios.org	Pleasefixtheiphone	No monetary incentive
		Preideas.com	Foursquare on Getsatisfaction	
		Easyjet on Getsatisfaction		
	Find Solutions	Cisco I-Prize	InnoCentive	Specific problem or challenge to be solved
		YTL myprize	NineSigma	Typically expert knowledge required
		Doritos crash the superbowl	Bootb	Monetary incentive for best solutions
			Idea-Bounty	
			Crowdspirit	
		Company	3rd party	
		PLATFORM OPERATOR		

TABLE 3: OPEN INNOVATION PLATFORMS. SOURCE: STOETZEL ET AL., 2011.[25]

Their classification lists platform examples for each cluster (it should be remembered that the study did not aim at the whole spectrum of open innovation platforms excluding, for example, business-to-business platforms or platforms with closed participation).

2.4 INNOCENTIVE

We here analyze a particular open innovation platform, InnoCentive, in greater detail. InnoCentive is an online platform for crowdsourcing innovative ideas and solutions to various challenges facing businesses, nonprofit organizations, or government

agencies. Challenges posted on the InnoCentive website deal with a broad range of issues such as computer science, chemistry, physical sciences, agriculture, and entrepreneurship. The company was founded in 2001 and is headquartered in Waltham, Massachusetts in the United States (US). It is home to a community of over 365,000 from nearly 200 countries that stand ready to help organizations devise innovative solutions to the challenges they face.[26]

This section of the report analyzes the InnoCentive platform in greater detail, listing the advantages and disadvantages of pursuing open innovation through this platform, and assessing its potential applicability to NDOs.

2.4.1 HISTORY

InnoCentive is the brainchild of a senior executive of Eli Lilly, a major American pharmaceutical company with over 40,000 employees all over the world and almost $20 billion in yearly net sales. Eli Lilly is one of only 3 US companies that consistently outperformed its industry competitors for more than 50 years.[27] In 2000, Eli Lilly's vice-president for R&D, Alph Bingham, had an idea that would radically innovate and transform the R&D process. Bingham's idea evolved around the notion that internal R&D processes are not able to capture the full potential of innovation. External innovators, even when working in unrelated fields, have the ability to provide innovative solutions that are not immediately considered by a firm. He emphasized the importance of being close enough to the field to understand the technical requirements but not so close that you are biased by the way those immersed in the problem tend to think.[28] Bingham thus decided to launch what is now known as InnoCentive: an online platform that matches organizations that are "solution seekers" with a wide array of potential "problem solvers". Firms facing specific R&D challenges can publish these on the InnoCentive website along with a prize award for those who are successful in solving the particular issue.

2.4.2 HOW DOES INNOCENTIVE WORK?

By connecting "seekers" and "solvers", InnoCentive tries to foster an environment of innovation in order to improve problem solving productivity.[29] By partnering with InnoCentive, organizations get access to InnoCentive's diverse solver community. The InnoCentive platform as such serves as an innovation hub that connects organizations that face a particular challenge and are searching for an innovative solution with individuals or organizations that have registered on the InnoCentive website and are attempting to find a solution to these challenges.[30] Today, the InnoCentive solver community has grown to more than 365,000 registered solvers from over 200

countries. Challenges are posted by corporations, governmental, and non-governmental organizations as well as a variety of other actors. For example, InnoCentive has partnered up with pharmaceutical companies such as AstraZeneca, governmental organizations such as NASA, and even with the US Department of Defense. Through dedicated innovation pavilions, partners can post their challenges to the public or they can decide to post challenges anonymously.

Depending on the challenge, InnoCentive and the seeker sign a terms of use agreement that defines the legal obligations of both parties to each other as well as those of the seeker organization to the solvers. Through this agreement, the solver's rights are protected. In addition, solvers are obliged to sign a specific terms of use agreement depending on the challenge.[31] In addition, both InnoCentive and the seeker organization work together in developing the challenges and formulating the problem statements. This is done through the InnoCentive Client Services Team (CST), which works not only with the Seeker organization but also with the solvers who might have questions related to the challenge. The CST is also able to work with organizations in case they need to post anonymous challenges in a way that would disguise the type of industry as well as the real nature of the posted challenge.[32]

InnoCentive offers a variety of products and services to its seeker organizations. The main products are the InnoCentive Challenge Programs, the InnoCentive@work software, and the InnoCentive Idea Management (IC IM) software. Depending on the specific innovation needs of the organization, it chooses to cooperate with InnoCentive on using one or more of the InnoCentive platforms. Through the InnoCentive Challenge programs, seeker organizations post their challenges on the InnoCentive website. There are several types of Challenges, such as the Ideation Challenge, Brainstorm Challenge, Reduction to Practice (RTP) Challenge, or the Theoretical Challenge and Electronic Request for Proposal (eRFP) Challenge. Organizations choose a certain challenge type based on their specific needs and requirements.

Organizations that are in need of a novel and creative idea and are still in the first stages of product development can opt for an Ideation or a Brainstorm Challenge. Both seek to provide a breakthrough idea or a creative solution to a problem; whereas the former is closed in format, the latter represents an open version of the former where solvers can interact with each other. In RTP Challenges, solvers have to present a successful prototype and prove that it works within the parameters and needs set by the organization. Theoretical Challenges constitute the same as RTP challenges, only they fall short of actually coming up with a prototype. They bring the idea closer

to an actual product or solution by giving a detailed theoretical explanation on why their solution will serve the organization best. In case a seeker organization is looking for a partner who has already developed a certain technology or has enough expertise to help develop it, then eRFP Challenges would be best suited for the organization.

The relation between the Seeker, Solver, and InnoCentive is determined on the basis of the Challenge type through the Terms of Use, the Challenge Specific Agreement (CSA), and other related documents. Through the CSA, which InnoCentive devises in collaboration with the Seeker organization, each challenge has different mechanisms regarding payment, dispute resolution, Intellectual Property (IP) transfer rights, etc. In most challenges, for instance, only InnoCentive and the Seeker are allowed to view the proposed solutions. However, in Brainstorm Challenges, solutions can be viewed by all participants.[33]

The CSA also decides the process of solution acceptance. In most cases, however, CSAs mention that the acceptance of a particular solution is the absolute and sole discretion of the Seeker and that merely meeting the predetermined minimum challenge requirements does not guarantee acceptance by the seeker.[34] The Brainstorm Challenge Terms of Use also mention that in cases where the seeker fails to notify InnoCentive with the selection of a winner, the latter is automatically chosen by the most votes in the Project Room community.[35] Depending on the challenge type and the CSA, the number of possible winners is determined. While some challenge types such as Theoretical Challenges only involve an award when challenge criteria are met, Brainstorm Challenges are guaranteed at least one winner. Conversely, eRFP Challenges do not involve cash awards but rather let winners negotiate the terms of the contract directly with the Seeker.[36]

Some CSAs specify dispute resolution mechanisms to be followed in case conflicts arise between a solver and InnoCentive. The arbitration procedure is subsequently administered by the American Arbitration Association in accordance with the Commercial Arbitration Rules.[37] In addition, CSAs can include exclusivity periods whereby solvers agree that their solution submission grants the Seeker the exclusive right to acquire the solution.[38] Other CSAs entitle Seekers to use material that has not been chosen as award winning solutions in case the material provided is similar to what a seeker already possesses.[39] To date there has never been an instance in which Seekers were found to have been in breach of IP law. According to InnoCentive, this also has to do with the fact that Solvers have to specifically identify the Seeker that stole their IP. The ability for Seeker organizations to remain anonymous prevents such

a case from occurring.[40] This effectively means that solvers will have less of a chance to know whether their solution has ultimately been used by the organization despite its official rejection. Solvers have little choice but to rely on the goodwill of the seeker organization and on InnoCentive and its technical capabilities to differentiate between successful and unsuccessful solutions.

Besides Challenges, InnoCentive also developed other products through which it could develop its partnerships with seeker organizations. A notable example thereof is the InnoCentive@work platform. The Innocentive@work platform offers partners the ability to incorporate the InnoCentive platform in a secure and cloud-based platform where challenges would only be available to a chosen private set of participants such as the company's employees, partners, or even customers. Organizations such as NASA and Eli Lilly have developed such a platform for their employees in collaboration with InnoCentive.

The InnoCentive Idea Management (IC IM) software is a social platform for idea management that InnoCentive developed in cooperation with NOSCO. It allows organizations to run idea campaigns, collect and share knowledge from employees and selected audiences in a structured way. Employees and invited audiences are then allowed to share their ideas, post comments, photos, and videos in a way that would allow the company to engage its employees and make full use of its idea generation potential.[41] By offering a customized innovation experience to seeker organizations through the InnoCentive@work or IC IM platforms, organizations can maximize the full potential of their employees without risking any of the adverse risks such as knowledge diffusion traditionally related to pursuing an open innovation policy.

In addition to the abovementioned products, InnoCentive also provides consulting and training services to organizations that are looking to invest in open innovation. InnoCentive's ONRAMP (Open iNnovation Rapid Adoption Methods and Practices) program provides training sessions for managers and employees in order to show how to effectively use the full potential offered by open innovation and ensure the success of its implementation.

2.4.3 WHO USES INNOCENTIVE AND WHY?

InnoCentive's platform 'InnoCentive@work' could be a valuable tool to organizations that prefer to operate through a platform that is not entirely open to outsiders. As a case in point, NASA has developed its own internal open innovation platform in collaboration with InnoCentive called NASA@work. NASA@work allowed NASA's

challenge seekers to post challenges that would only be available to NASA employees across its 10 field centers without the risk of knowledge leakage. It also helped in fostering a collaborative environment across NASA's field centers (for more information on how NASA engages in open innovation see 2.5.3).

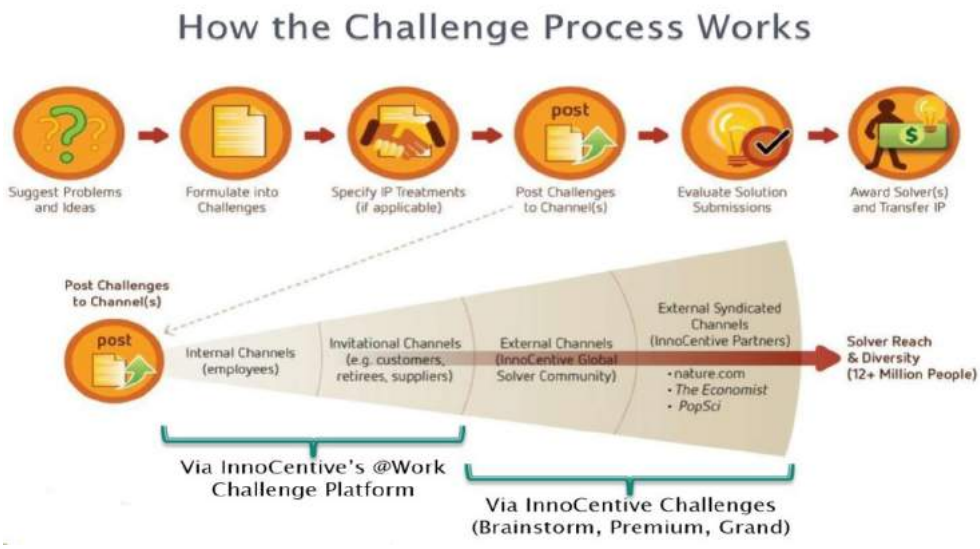

FIGURE 3: THE INNOCENTIVE@WORK TOOL. SOURCE: FRANKLIN, 2013.[42]

Figure 3 shows a schematic overview of how the InnoCentive@work functions and how NASA uses it within the organization. It demonstrates a best-practice approach where NASA challenge seekers initially opt for an internal challenge through NASA@ work in order to either find a solution, or at least fine-tune a challenge topic, and then follow it with an open challenge through one of the external open innovation platforms.

2.4.4 BENEFITS OF USING INNOCENTIVE

The InnoCentive platform can offer substantial returns to corporations looking to invest in open innovation. The costs associated with partnering up with InnoCentive, posting a challenge, and receiving a solution are much lower than the costs associated with traditional modes of R&D. InnoCentive's awards normally range between $5,000 and $1 million, which is a fraction of what is generally spent on a traditional R&D process.[43]

Another reason why organizations would choose to work through InnoCentive is that it broadens the solutions space, including those solutions that would be considered to

be too unorthodox within the organization itself. The speed by which new innovative solutions can be found also serves as a pull factor. By being able to tap into a much larger pool of potential problem solvers, challenges that a company normally spends years on solving through its traditional R&D process can be solved in a matter of months.

Furthermore, making use of InnoCentive fosters an innovative culture, opening up the organization to accepting new ideas and working with external partners. It benefits the employees of the seeker organization by advancing their ability to frame research challenges. Employees are then able to use these new skills in other areas of their work. The organization benefits from a smoother IP transfer process by having InnoCentive deal with any legal issues. This means the organization has more time to work on research and spend less on IP lawyers.[44]

2.4.5 RISKS OF USING INNOCENTIVE

An organization might face a backlash from experimenting with open innovation owing to cultural resistance. Most in-house R&D professionals are used to spending time on challenges and have pride in coming up with their own solutions. This drive is an invaluable asset to an organization. Open innovation as the main innovation mode in an organization would fundamentally change the role of R&D professionals: from problem solvers to problem formulators in search of solution seekers.[45]

Another important issue that has to be dealt with when introducing open innovation practices is knowledge diffusion. Although open innovation allows you to tap into a vast pool of resources, it also exposes the organization in the sense that competitors may know what you are planning and tailor-made solutions can become available to opponents.

2.4.6 RISK MITIGATION

As mentioned in the previous section, InnoCentive limits the risks of knowledge outflow by offering the option of anonymity to the Seeker organization and letting the company decide whether it wishes to reveal its name. InnoCentive also cooperates with the Seeker during the problem formulation process in order to hide the true nature of the problem, as well as the organization's industry. This assures InnoCentive's partners that their competitors, or otherwise unwanted actors, do not get their hands on information that the organization prefers to have under its control.

The development of the InnoCentive@work platform further mitigates the risk of knowledge outflow. Organizations that are hesitant in acquainting the public, and their competitors, with their current problems and knowledge gaps would be able to open up the process as they deem appropriate. By using an invite-only platform, companies can choose who to share their challenges with (employees, customers, or partners), thus minimizing the risk of knowledge outflow.

InnoCentive's partnership with the Seeker organization could also help with the mitigation of internal organizational risks such as cultural resistance. The ONRAMP service and the open innovation workshops provided by InnoCentive to the Seeker organization are available to anyone in the organization, from executives to challenge owners. These workshops aim to ingrain a culture of open innovation into the organization and align the views of stakeholders regarding the importance and benefits of open innovation. This ultimately facilitates a smoother adoption of open innovation practices.

Seeker organizations can also pursue risk mitigation practices. To mitigate the problem of open innovation resistance, NASA's Human Health and Performance Center established the Solution Mechanism Guide (SMG), an online tool developed through another open innovation challenge. The SMG helps employees in selecting a project management approach which would work best given the resources and needs of this specific project.[46] It gives employees the opportunity to use both traditional as well as open innovation tools so that the most efficient mechanism would be recommended. Employees can use the SMG in two main ways. First, the SMG acts as a filtering mechanism. By entering the parameters of a certain problem, the SMG filters the solution mechanisms to meet the criteria. Thus, the employee is better informed about which external or internal platform to use for his challenge. Second, the SMG also acts as an educational and training tool for employees. Through the SMG, employees can view past case studies and user experiences and learn new tips and tricks on using a particular solution mechanism.[47]

The use of a platform such as SMG has several benefits: it improves communication within an organization by speeding up the process of information dissemination; it increases employee awareness regarding the utilization of different solution mechanism tools; it reduces the time needed to solve problems; and it empowers employees. SMG thus contributes to the creation of an organizational culture that is collaborative and amenable to open innovation platforms.[48]

2.5 NEW FORMS OF OPEN(ISH) COOPERATION IN DEFENSE

The processes whereby NDOs define their capability needs and then ensure access to those capabilities remain one of the most difficult – and controversial – aspects of what some call the "defense enterprise". In the past decade – and especially since the advent of austerity – value for money has become one of the foremost battlefronts of defense transformation. "Big A" (the main weapon platforms for sea, land, and air) acquisition has been at the heart of this battle. Many of the problems in this area are fairly well understood.[49] But even the most advanced NDOs (e.g. the United Kingdom and the US) keep struggling to come up with effective solutions.

One of the fundamental problems with the Big A acquisition process in many NDOs lies in the earliest stages when defense requirements are defined. For most of the Cold War, the main drivers of the requirements-setting process were the services NDOs provided: they were responsible for training and equipping the troops. Because of the many fragile political compromises this entailed – both within as well as across the services – nobody really had any incentive to rock the boat. This also meant that the interaction with the outside world (including the private sector) was preferably as closed as possible, with a small number of preferred, strategic partners that could be trusted to stay in the box. The actual permeability of this process to outside influences varied with the particular "political economy" of defense in various countries,[57] but most countries found it extremely difficult to avoid collusion effects.

The past few decades brought three main changes to this situation. The first one was that most NATO countries moved towards a more joint process of defining requirements. This already led to more internal openness. These countries, secondly, also strengthened the walls between the requirement setting stage and the subsequent procurement stages in which tenders are issued, competing offers are assessed and adjudicated, and the actual procurement process is set in motion. The hope was that by sheltering the requirements setting process from untoward influences, the "defense enterprise" would better be able to decide for itself what it really needs, unencumbered by external pressures and/or conflicts of interest. The third major change was that, under pressure of ever more demanding publics and parliaments, the NDOs gradually also became somewhat more transparent in what they divulged about all of these choices.[50] Here, too, the hope was that this increased openness would lead to sounder balance-of-investment choices.[51]

Reality, alas, proved more recalcitrant. The dynamics between the services did not really disappear and the early stages of the requirement setting process became in

some ways even more bureaucratic and (because of its isolation) inward-looking. Rather than going for 'better together (with others)', the process arguably became 'worse alone (amongst ourselves)'. This more insulated approach had two negative consequences. First, outside inputs (and – often – reality checks[52]) were weak or absent. And second, the main players (the services) engaged in even more "logrolling" (trading favors: "I'll give you your pet toy, if you let me have mine"). So whereas the taxpayer was supposed to benefit from these changes, it is far from clear that she did.

A few countries have been trying quite diligently to remedy this unsatisfactory situation. And one of these interesting innovations in this area lies in the very early stages of the Big A acquisition process that we already alluded to as being critically important. The main idea here is to combine some of the strong points of the old system with some of the strong points of a less insular and more open system. Rather than drawing rigid lines between defense and non-defense, these new forms of somewhat more open cooperation between the private and the public sector try to come to a new equilibrium that may stand a better chance of providing the taxpayer with a better value for money proposition. In the very early stages of the process, the – in InnoCentive terms – seekers (in this case Defense) and the solvers (in this case the defense solution providers) jointly try to specify how a certain need could theoretically (pre-competitively) be met. This changes the decision-making dynamics by opening the process up to the outside. It gives Defense the advantage of being able to benefit from the often superior knowledge in the private sector about how problems can be solved in the process of defining the requirement. Based on this pre-competitive, pre-political, pre-bureaucratic stage, Defense can then decide on its own what it wants to do in the next (still sheltered) stage. But it will now, such is the logic, be able to do so on a more informed basis. All of this is not based on backroom deals or old boys networks but rather on a (relatively) level playing field and at least some dispassionate analysis.

To the best of our knowledge, there are three countries that have experimented with this model. The UK, really a trailblazer in acquisition reform,[53] was an early adapter through its "NITEworks" facility, which dates back to 2003 and is still going strong. The distinguishing feature of this new form of cooperation between the private sector and the public defense sector is that it is spearheaded by a national champion (BAe SYSTEMS). In 2005, the Australian NDO stood up RPDE, an Australian facility in Canberra that was inspired by NITEworks. The basic philosophy is the same but the kind of work undertaken is somewhat different as is the way it is set up. With NITEworks, the MOD uses BAe SYSTEMS as a prime to provide the physical

infrastructure and to engage the other organizations through subcontracts. In the case of RPDE, the Australian government provides the infrastructure, seconds an industry executive as the head, and has a contract directly with every member company. RPDE has many more members than NITEworks, including some one-man bands who only work for/at RPDE. In 2007-2010, Canada experimented with a similar model; however, it ultimately failed.

2.5.1 NITEworks (UK)

In 2003, the UK Ministry of Defense launched NITEworks, a partnership initiative that spans the UK defense sector to help improve decision making on requirements setting. As outlined in the 2005 Defense Industrial Strategy, NITEworks "was established to provide an integration and experimental environment to assess the benefits of Network Enabled Capability (NEC) and the options for its effective and timely delivery".[54] However, NITEworks' remit was not strictly limited to NEC since work focused on both the network and information flows. NITEworks received an initial 5-year £47 million Assessment Phase contract, which was renewed in 2008 for another 5 years. In this second contract, the area of interest was widened. MOD specified the following priorities: support to frontline operations, capability improvements, and enhancements and acquisitions decisions. The MOD also had the organization adopt a more competitive business model, attracting funds from across the MOD rather than reliance on a single MOD funding line. Considerable weight was given to achieving value for money.

In addition to the MOD itself, NITEworks consists of twelve UK defense industry companies, as well as more than 130 Associate Organizations. Companies that have capabilities that could be of use to the defense sector can apply for membership. Once accepted, they have access to all partnership communication, workshops, and activities.[55] NITEworks has a core staff of 37, drawn from the military, MOD civil service, the Defense Science and Technology Laboratory (Dstl) and industry.

Working together with defense industry and academia to analyze problems and look for solutions, the MOD claims to be better informed about what the solution space may actually look like and to select solutions that offer excellent value for money. The partnership also allows the MOD to "de-risk and accelerate the provision of military capability."[56]

How does NITEworks actually work? MOD staff can post particular challenges on the NITEworks platform after internal communication with NITEworks' Stakeholder Management Team (SMT). Only challenges where "benefit is gained from the use of a

pan-industry/MOD partnership"[57] can be posted on NITEworks. The SMT then works together with the MOD sponsor[58] to formulate the problem question. This is followed by the development of a business case to finally determine whether the NITEworks platform will be chosen. Subsequently, a role request is issued to NITEworks partners and associates who subsequently apply to join this specific challenge. At the end of the selection process, a small and focused team consisting of defense and industry experts is selected. The team then starts refining and defining the scope of the problem question. The overall process takes on average six to eight months to finalize and deliver the final product.[59] When it comes to IP provisions, the British Crown retains all IP rights and only issues licenses for partners to use the knowledge for the Crown, not for commercial use. Associates can only access an executive summary of the output, not the output itself. However, they can still access work in which they directly participated.[60]

To date, NITEworks projects have dealt with a wide array of fields including logistics and sustainability, increasing open source intelligence capabilities, improving aviation simulation, as well as cybersecurity. In 2010, as part of the Strategic Defense and Security Review, the MOD sought to plan for the future of equipment priority in order to ensure "resources are directed to the most urgent areas."[61] A small NITEworks team was assembled and joined the MOD team tasked with developing the plan. The team suggested novel ways of campaign planning based on a color-coded bullseye chart (see Figure 4) that basically enables employees to "indicate the level of capability available at different points in time."[62]

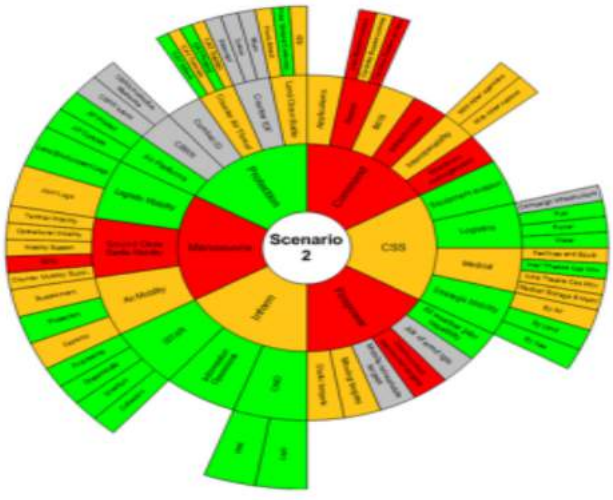

FIGURE 4: COLOR-CODED BULLSEYE CHART. SOURCE: NITEWORKS, 'ARMY EQUIPMENT DEVELOPMENT PLAN (AEDP), 2011.

One of the largest projects ever undertaken by NITEworks is *Talon Strike*, a project aimed at enhancing battlefield interoperability between UK and US forces. After operations in Afghanistan, both countries realized the necessity of seeking more efficient information sharing and shared situational awareness capabilities. Thus, in 2008 a NITEworks team led by the MOD was assembled. In addition to the MOD and Dstl, the team also included NITEworks members such as BMT Hi-Q Sigma, Finmeccanica UK, Fujitsu Services, General Dynamics UK, Northrop Grumman UK, QinetiQ, SyntheSys Systems Engineers, Systematic Software Engineering, Systems Consultants Services, and Thales UK.[63]

NITEworks organized a conference in Farnborough, which was attended by UK and US war fighters. In addition to deciding on the command and control systems to be used during the exercise, the conference narrowed down the focus of the project and specified it to a "shared situational awareness, a common operational picture and a dynamic collaborative planning environment."[64]

NITEworks' task was then to work with the Command and Control Development Centre to develop a set of systems that enable information sharing including positional information, orders, and other information vital for battlefield operations. Based on these results, a two week joint exercise took place between US and UK forces where the latter were accompanied by the NITEworks team in order to aid in operational analysis and other complex technological tasks.[65]

The *Talon Strike* project ultimately led to a reduction in the risk of friendly fire incidents, helped in de-risking future requirements, and proved to the MOD the importance of understanding challenges emanating from interoperability and integration of Command and Control.[66]

The UK MOD's commitment to NITEworks was reconfirmed on July 30th, 2013 with the award of a £17 million, three-year MOD contract,[67] and on September 17, 2015, when the contract was extended until March 31, 2018[68] with the following statement: "the NITEworks approach enables the MOD to rapidly assemble expertise in an impartial environment, with access to prior knowledge and industry Intellectual Property from across the defense community. It brings together knowledge of the problem and solution space which both enables a better understanding of the feasibility of recommendations and allows them to be rigorously tested and challenged from a range of perspectives – blending incumbent knowledge with the fresh thinking of new suppliers – be they generated by SMEs or a global company."

2.5.2 RAPID PROTOTYPING, DEVELOPMENT AND EVALUATION PROGRAM (AUSTRALIA)

Similar to NITEworks, the Rapid Prototyping, Development and Evaluation Program (RPDE) is a partnership program between defense, industry, and academia, developed by the Australian MOD. It specifically deals with complex, high-risk capability problems that have a significant integration component. The solutions sought by RPDE are focused on accelerating the delivery of the Australian Defense Force's (ADF) war fighting capability through collaborating with defense industry and academia to support innovative solutions.

RPDE basically performs two types of activities; Quicklooks and Tasks. As a first step, a Quicklook is done by rapidly assembling a team through RPDE partners who submit a report on a certain defense capability issue usually within a three month timeframe with the aim of providing advice and guidance. Secondly, Tasks aims to deliver a prototyped solution in 12 to 18 months. These solutions could range from reports to proofs of concept or even physical prototypes.[69] Figure 5 shows the lifecycle of RPDE tasks.

FIGURE 5: LIFECYCLE OF RPDE TASKS. SOURCE: RPDE, 2013.[70]

Usually, RPDE Tasks finish at the Solution Development phase. However, in some cases RPDE can provide assistance in the implementation of the solution. As one example, an RPDE team was assembled to develop options for the provision of a digital hydrographic system. During the Solution development phase, the sponsor faced an urgent operational need to develop a Maritime Classified Geospatial Data Management System (MCGDMS). To deal with such an urgent need, the team developed a de-risking proof of concept and subsequently moved to the solution development phase in March 2013. Finally, in December 2014 the required outcome was delivered to the challenge sponsor.[71]

Another successful example was the development of a personnel-borne Improvised Explosive Device (IED) detection device. The Counter Improvised Explosive Device

Task Force (CIEDTF), who the sponsored this Task, was looking for a device that would be able to enhance ADF personal protection in combat zones by detecting whether an individual might be wearing an IED device. In 19 months' time, a successful solution was prototyped and developed. Starting with the Question development phase, the CIEDTF proposed the following problem question: "Can standoff IED detection technology be miniaturized and a concept demonstrator be developed to enhance personal force protection for soldiers from IEDs?" During the Discovery Phase, the task team analyzed worldwide technology related to IED detection capabilities and identified options that could be pursued based on several technological, size, and financial criteria. Subsequently, RPDE issued an Invitation to Register (ITR) to all RPDE participants. Shortlisted candidates were then asked to present their proposals. The proposal provided by Tactical Research Pty Ltd. was accepted, and upon authorization from the One-Star steering group, RPDE entered into a contract with the chosen organization. Through collaboration between RPDE and Tactical Research, a handheld IED detection system was developed and successfully tested in July 2014.[72]

2.5.3 NASA (US)

Open innovation within NASA falls under the Open Government Initiative, which aims to create "a new level of openness and accountability in [NASA's] policies, technology, and overall culture."[73] The latest open government plan emphasizes the encouragement of collaboration and innovation both within the agency itself as well as externally by enabling citizen participation and encouraging partnerships that have economic opportunity potential.[74]

In 2005, NASA launched the Centennial challenge program seeking to offer prizes to individuals and small businesses that successfully solved NASA challenges. A year later, however, NASA faced far-reaching budget reductions. This effectively meant that several ongoing projects were either delayed or scrapped altogether.[75] R&D units inside NASA had to find new innovative and cost-effective practices to mitigate the negative effects of budget cuts. Several reports and strategies were published to that effect including the May 2007 strategy,[76] the Augustine Committee report,[77] and a 2009 benchmark study,[78] all of which emphasized the importance of finding new ways to advance NASA's mission with the limited resources at hand. Historically, NASA relied on internal research and development. The new 2007 strategy, however, emphasized collaboration by developing strategic partnerships both internally with other US government agencies, as well as externally with international partners, academia, and commercial entities. The strategy also aimed to address traditional perceptions inside the organization that did not align with proposed strategic change,

such as risk aversion, civil servant superiority, or the perception that everything can be done by NASA itself.[79]

The outcome of these strategies was the awareness that a new open innovation model had to be introduced within NASA. The Space Life Science Directorate (SLSD) took the lead role and decided to tryout three open innovation platforms, namely InnoCentive, Yet2.com, and TopCoder. Workshops were then designed and given to SLSD members by the three organizations. From 2009 to 2010, 11 R&D units put forward 14 problems on the open innovation platforms. Seven challenges were run on InnoCentive six on yet2.com, and one on TopCoder. The results were beyond expectations as all seven InnoCentive challenges proved either solved or partially solved. Out of the six challenges run through Yet2.com, one provided a novel solution, while the others had either generated ideas that could be incorporated for further development or had helped identify partners with whom NASA could work on solutions. The result of the TopCoder challenge was incorporated into an existing NASA medical database.[80]

In one particular challenge posted on InnoCentive, NASA sought an algorithm that would solve a 30 year old problem concerning data-driven forecasting of solar events. The solution required was supposed to forecast solar events four to 24 hours in advance with a 50% accuracy and a two-sigma confidence interval. Bruce Cragin, a retired radio frequency engineer, was able to find an algorithm that exceeded NASA's expectations. His algorithm was able to predict solar events eight hours in advance with 85% accuracy and a three-sigma confidence interval.[81]

Following the success of the pilot program with the external innovation platforms, NASA decided to build a new internal open innovation platform in collaboration with InnoCentive. This platform, called NASA@work, was similar to InnoCentive but open only to NASA employees. The idea behind it was to capture the full innovation potential of NASA. For NASA, as a large organization with thousands of employees, this meant that a challenge faced by an individual employee in one field center could now be accessed and solved by anyone in the agency without resorting to InnoCentive public Challenges. At the same time this would foster collaboration within the organization, help in team-seeking, and make use of employee diversity.[82]

Through Yet2.com, another online open innovation platform that acts as a technology scout, NASA has been able to find future collaborators that are not immediately on its radar. After NASA posts its technological needs, Yet2.com looks into its worldwide

network of specialists, runs competitions, and finds the most suitable partners from which NASA can subsequently choose who to collaborate with.

This means that NASA has adopted a flexible open innovation strategy. It moves between a closed participation platform such as NASA@work and an open one through InnoCentive and from an open platform – albeit more limited in scope – such as Yet2.com back to a closed one with its chosen collaborators, depending on the stage of the innovation process it finds itself in.

Still, NASA's adoption of open innovation was not without problems. In some cases, NASA's efforts at involving the public through different open innovation platforms found little success. Some Centennial challenges had to be closed without finding a clear winner. This was the case for the Strong Tether Challenge, which sought the development of components related to building a Space Elevator, yet ended up without declaring a winner.[83] The fact that the tether is made out of expensive carbon-nanotube material complicated the task of even finding competitors to enter the challenge; something that was hard to change no matter how high the prize money was.[84] The MoonROx Challenge suffered a similar fate in 2009 after no competitors even registered for the challenge due to its difficulty as well as the absence of any commercial potential. After seeking a way to produce breathable Oxygen from materials commonly found on the moon, the Challenge had to close and the prize of $1 million went unclaimed.[85]

Furthermore, the space agency found that not everyone within the organization viewed the adoption of open innovation positively. Some R&D professionals feared that their identity was threatened by open innovation. They believed that looking for solutions externally meant that they are no longer valued within the organization. There were also those who showed acceptance of open innovation practices, yet were in fact against it. To satisfy their managers, they simply opted for open innovation in strategically unimportant challenges and kept the more important ones for internal consideration. Sometimes, they withheld valuable information gained through open innovation platforms. The traditional identity of a smart problem-solver was thus threatened with the advent of open innovation and the accompanying new identity of a solution seeker. This meant that the perception of NASA as a place that allows its engineers to access, plan, and solve a problem was shattered. In fact, some even saw the idea of looking for external challenge solvers as cheating. This kind of cultural resistance can indeed pose a risk to organizations that view open innovation as a strategic objective.[86] Looking back, Lifschitz-Assaf (2015) found that the external

experts and managers who introduced the concept of open innovation to NASA focused primarily on the time and cost efficiency of the model and overlooked the organizational aspects and the adverse effects on R&D professionals. This in turn exacerbated the perception of identity threat to the employees.

2.6 APPLICABILITY FOR NDOs

Many of the advantages that have brought private companies to embrace the open innovation paradigm also hold for NDOs. Tapping into a (vastly) wider pool of experts than those within immediate reach is essential to maintain a technological edge in a world where ideas and solutions easily spread and western military superiority is no longer a given. Cost efficiency and better value for money are as important for military organizations as for private companies in light of budget constraints and scrutiny over the spending of taxpayers' money. Time efficiency, i.e. faster delivery of innovative solutions to particular problems, is also an issue in the military realm. This holds true in particular for actual missions confronted with an emergent challenge (such as the challenge of detecting improvised explosive devices posed in the Iraq and Afghanistan campaigns). Finally, the fact that embracing open innovation practices contributes to creating and stimulating a culture of innovation – as part of a more general culture of agility – probably also holds true for NDOs.

NDOs traditionally put a high premium on secrecy and have therefore tended to prefer closed modes of innovation. To some, the very notion of open innovation even contradicts the fundamental principles by which NDOs function. It is important to bear in mind, however, that secrecy is not a goal in and of itself. The real goal is to forge an attractive (security) value for money proposition that reliably safeguards the stakeholders' (countries' taxpayers) security at an affordable price. In this sense, NDOs do not differ all that dramatically from their public or private sector counterparts. Protecting one's crown jewels is vitally important to many private companies that may have billions of investments at stake. This is, for instance, the case in the pharmaceutical industry, which nevertheless is increasingly broadening its cooperation portfolio with elements of open innovation.

In this case study, we have particularly looked at InnoCentive as an example of an open innovation platform. The available evidence on InnoCentive illustrates both the first-order potential of such innovation malls and the risk mitigation strategies that both solution seekers and InnoCentive as an organization have resorted to in their interaction. The InnoCentive platform is developed in a way that allows the seeker company not only to post challenges anonymously but also to work with InnoCentive

in order to hide the true nature of the challenge and the industry involved, thus benefiting from open innovation while minimizing the risk of unwanted knowledge outflow.

In addition, there are ways to capture the value of open innovation without risking knowledge outflow, for example by investing in the InnoCentive@work or the IC IM platforms. In big organizations such as NDOs, the number of employees involved is often huge and they are most probably geographically spread out in different branches. The experience of NASA suggests that in such cases, an internal open innovation platform such as NASA@work captures the full potential of innovativeness inside an organization before an external challenge is required. In the case of NDOs, investing in such a platform could prove useful even if it is decided that internal challenges shall not be succeeded by external ones.

Although it is fruitful to mirror NDOs with the corporate world and their respective processes and value chains up to a point, a defense organization is not a business. *In ultimo*, the failure of NDOs to perform in the face of "competitors" may put vital national interests and even the very existence of the state in jeopardy. This is quite different from the workings in the commercial market place, in which the rise and fall of individual companies is part and parcel of a continuous process of creative destruction. Maintaining a competitive edge vis-à-vis (potential) adversaries, particularly for western NDOs that have technological superiority engrained in their modus operandi, is a far cry beyond achieving a temporarily "first market entry" advantage. MODs therefore strive to keep the exact specifications and even performance range of their core capabilities hidden (*"mil specs"*), both to deny possible opponents the same possibilities and to make it more difficult for them to design adequate counter-measures.

In addition, in particular for IT-heavy systems, information security is a crucial issue.[87] Defense organizations need to be fully aware of liabilities and vulnerabilities in their systems. At the same time, this information must be kept secret from potential adversaries as much as possible.

Furthermore, the (existing) military capability portfolio of NDOs is to a large extent built around a limited number of main weapon platforms, such as frigates, tanks, or fighter jets. Such large platforms remain in service for decades without major changes to the platform itself (hull / frame / chassis). This is in contrast to many of the components, which are not only carried as components of the platform but also

increasingly derive their functionality from software. It becomes meaningful to look upon some, possibly many, of these modules as applications that adhere to the much faster pace of IT-innovation. One of the big challenges for NDOs is to combine these dynamics into system integration processes that harness fast innovation at the component level in continuous performance improvement while retaining the structural integrity at the systems or systems-level.[88] Typically, effective system integration requires close corporation between a NDO and a handful of corporate system integrators.

A critical factor for NDOs to be able to unleash open innovation's full potential is to simultaneously organize and promote a process of functional decomposition and functional integration. On the one hand, the functionality of defense systems and processes must be split into clearly distinct modules that have maximal internal consistency and minimal external coupling. The interfaces between these modules, describing their functional interaction, should be standardized and open. Such a decomposition renders it possible to distinguish between core mil spec modules and modules that may be developed and acquired on the open market; furthermore, this allows for describing the latter in terms of their external behavior rather than their internal workings. This is the basis for being able to use the kind of open innovation platforms that InnoCentive exemplifies.

On the other hand, individual modules must also be easily clustered into an integral capability. This system integration is a dynamic process: according to momentary needs, it should be possible to add or withdraw modules in a plug-and-play fashion to generate a custom-made capability best fit to perform the mission at hand. The way in which mobile device owners create their own unique functional environment through the Apple iStore and Google Play platforms gives a vivid image of how functional decomposition (myriads of apps) and integration (clustering apps on a single mobile device, with some apps working closely together with some other apps) can meet.[89]

Finally, there is the issue of cultural resistance to open innovation in general. Defense organizations are known for having a comparatively high degree of resistance to change. Small, relatively inexpensive pilot projects using platforms such as InnoCentive may serve as eye-openers and track record cases to promote open innovation. Again, NASA can serve as an example. To mitigate the problem of open innovation resistance, NASA established the Solution Mechanism Guide (SMG), an online tool developed through another open innovation challenge. SMG helps employees in selecting a project management approach that would work best given the resources and needs of

this specific project.[90] It gives employees the opportunity to use both traditional as well as open innovation tools so that the most efficient mechanism will be recommended.

2.7 PRACTICAL EXAMPLES

US security and defense organizations have been especially interested in pursuing partnerships with InnoCentive. Since InnoCentive started, US governmental agencies have signed a total of nine contracts with InnoCentive worth $6.34 million,[91] with the Department of Defense being the most invested partner. Other NDO partners in the US include the Department of Interior and the Department of Homeland Security.[92] Even the Department of State has launched several Challenges using the InnoCentive website, most notably one relating to innovation in arms control.[93]

In 2013, the Defense Threat Reduction Agency and the US STRATCOM Center for Combating Weapons of Mass Destruction posted a challenge seeking an algorithm to analyze a sample of DNA in a rapid manner to help protect US personnel from bio threats. The winning team of three scientists from Germany and Singapore were able to find an algorithm that reduced this time from weeks to tens of minutes, thus enabling the treatment of personnel in the field.[94]

In addition, the Combating Terrorism Technical Support Office (CTTSO) has its own innovation pavilion on InnoCentive and has given awards to several challenge solvers. In one challenge, the CTTSO sought to address the ineffectiveness of screening out individuals predisposed to violence through a non-invasive method to predict violent behavior within society.[95]

Currently, the use of open innovation malls such as InnoCentive for NDOs seems to be limited to the sub-system level and non-mission critical components. (Better) use of open innovation platforms at this level could well be organized as an integral part of the supply chain of defense system integrators. As NDOs and system integrators gain experience in specifying functionality in a modular fashion, the use of open innovation platforms may multifold and possibly move up from the component level to the system and even system-of-systems level.

For more sensitive components, NASA's experience suggests that semi-open innovation mall mechanisms within a more controlled environment of trusted innovation partners is possible and potentially useful. An important lesson is that open innovation does not necessarily take place in a static form but could be dynamic,

moving between open and closed forms of cooperation. Companies that adopt dynamic open innovation have the ability to maneuver from open to closed forms and vice versa. Some developments in the InnoCentive case also point toward minimizing the risk of unwanted knowledge outflow while retaining the benefits from open innovation. The platform has developed mechanisms to allow the seeker company not only to post challenges anonymously but also to work with InnoCentive in order to hide the true nature of the challenge and the industry involved. An important lesson is that companies that adopt dynamic open innovation have the ability to maneuver from open to closed forms and vice versa. In particular, the closed-open-closed approach that NASA has tested – starting from a closed form of cooperation, followed by an open one, and then back to a closed form – might prove a valid template also for NDOs.

NDOs could also benefit from cooperation with InnoCentive in crisis situations and natural disasters. "Fast track innovation and procurement" processes may serve to fill an immediate operational gap or requirement in the context of ongoing missions. In many instances, an early response is paramount over secrecy, rendering innovation malls a possible instrument of choice. As an example, after the 2010 oil spill in the Gulf of Mexico, InnoCentive ran an emergency response challenge to assist British Petroleum (BP) in the remote sensing of oil and skimming technology. Although BP ultimately decided not to look into InnoCentive's proposals,[96] the ability of the InnoCentive community to address complex technical challenges in the event of natural disasters could potentially be of use to government agencies tasked to deal with their aftermath.

3 CASE-STUDY 2 – THE HACKER COMMUNITY

3.1 WHITE AND BLACK HAT HACKERS 57
3.2 COOPERATION BETWEEN HACKERS 58
3.3 COOPERATION BETWEEN NDOs AND HACKERS 61
3.4 BENEFITS OF COOPERATION 65
3.5 RISKS AND CHALLENGES 66
3.6 MODELS OF COOPERATION 70
3.7 APPLICABILITY FOR NDOs 72
3.8 PRACTICAL EXAMPLES 74

3 CASE-STUDY 2 – THE HACKER COMMUNITY

3.1 WHITE AND BLACK HAT HACKERS

The 2007 distributed denial-of-service (DDoS) attack against Estonia, the 2008 cyber-attacks against Georgia in the run-up to the Russian invasion, and the use of the Stuxnet worm against Iranian nuclear facilities in 2010 are just a few examples of high-impact cyber-attacks where state support is strongly suspected. The Sony hack and WikiLeaks' NSA-spying revelations are other examples of high impact internet-related crimes that could be interpreted as acts of war in disguise. Despite the fact that these were criminal offenses, some of these actions, notably the Wikileaks revelations, have received some respect from the general public. Hackers are sometimes viewed as "online freedom fighters", exposing injustice and wrongdoing.[97] Stories of hackers who get hired after a successful hack are plentiful.[98] Hacking is hot. More importantly from the point of view of this report, the use of hacker communities represents in many ways novel ways of cooperation that can prove to be successful for state actors.

A hacker can be defined as someone who seeks and exploits weaknesses in computer systems and networks. Some hackers are looking for vulnerabilities to help companies or governments, so called "white hat" hackers.[99] Most hackers, however, use their skills for their own benefit (or just amusement) and no-one else's: so-called "black hat" hackers or, in short, black hats. A black hat hacker who finds a new security vulnerability may sell software exploiting it (an "exploit") to criminal organizations on the black market or use it to compromise computer systems. Black hat hacking occurs in varying degrees of severity: whereas some hackers might be motivated mainly by solving technical challenges or by political or social goals (i.e. "hacktivists") and only involved in relatively minor crimes, others perpetrate serious criminal activities, such as hacking banks to steal money or by paralyzing critical infrastructure. The divide between black and white hats is not always strict: there is also a group of "gray hat" hackers located somewhere between the two. Gray hats do not necessarily work for personal gain, but they might technically commit crimes or perform unethical activities as well.

Whereas white hat hackers are usually employed by computer security companies,[100] black hat hackers will often go to great lengths to remain hidden. They form secret communities and shadow markets. Thus, two forms of cooperation with hackers can be distinguished. First, cooperation within the hacker community itself, or "horizontal cooperation" (see Section 3.1). And second, cooperation between NDOs on the one hand and hackers on the other, or "vertical cooperation" (see Section 3.2). For our purpose, the latter is obviously interesting. But this also applies for the former: knowledge of how hackers cooperate among themselves, how they establish trust, and why they act in the way they do could help NDOs in their own quest for more effective forms of cooperation with more diverse groups of partners.

3.2 COOPERATION BETWEEN HACKERS

In Hollywood, hacking is often portrayed as the activity of a lone individual who attacks major companies from his/her home.[101] In reality, committing serious cybercrimes typically requires cooperation between numerous individuals who often do not know each other and have never met each other in person. This makes searching for potential partners and establishing cooperation in cyberspace a challenging task. Since anonymity is a central part of the online environment, it is difficult to determine who you can trust: putting your trust in the wrong person may lead to being exposed to the authorities.[102]

3.2.1 INCENTIVES FOR HACKERS TO COOPERATE

Incentives to cooperate in cyberspace (versus operating alone) are essentially the same as in other fields of human activity. However, there are some peculiarities that are related to the specific features of the Internet and the illegal nature of, at least, a large part of such cooperation. First of all, working together can increase the benefits (and lower the costs) of a cyber-attack. In some cases, involving more people can increase the direct effect of the attack. This is especially true for DDoS attacks, where scale is essential for success. An example is the 2007 attack on Estonia, which paralyzed the country for three full weeks. Here, a group of Russian activists was furious with the Estonian decision to move a Soviet World War II memorial in Tallinn.[103] Such a large-scale attack is difficult to conduct for a single hacker.[104]

Another strong reason to cooperate is provided by the benefits of specialization. Participants in the underground cyber economy play different roles. Some provide tools for cyber-attacks (exploits, malware, botnets, etc.) or even provide cybercrime as a service. Others offer auxiliary and intermediary services. These include administrators of black markets and mules (who move money or illegal goods from one place to

another).[105] Specialization and the existence of sophisticated black cyber markets lowered the technical barriers to commit cybercrime and as a result expanded the number of people and groups engaged in criminal cyber activity. The same factors also reduce the risk of the final beneficiaries of the crimes being caught because identifying them requires tracing the numerous steps that were involved in a cyber-attack. Easy availability of cybercrime-related tools and services enable a much higher sophistication and complexity of attacks, thus greatly increasing their rewards.

Finally, in case of hacktivism (e.g. Anonymous and some other groups), next to the obvious advantage of scale, hacking together might give the sense of a being part of a group with a mission, or a reassuring feeling of justification.[106] An example is the recent hack on the Ashley Madison website, an online dating site that helps people to cheat on their partner. A group of hackers referring to themselves as 'The Impact Team' hacked the website, stating that the site should go offline or the data of all the customers would be made public. A few days later, when Ashley Madison refused, their data was indeed posted on the Dark Web: 36 million accounts, including names, heights, weights, genders, addresses, email addresses, GPS co-ordinates, credit card transaction details, and sexual preferences were made public. The hackers accused the users of "fraud, deceit and stupidity," telling those affected to "learn your lesson and make amends".[107]

3.2.2 ENSURING QUALITY AND TRUST

The success of the above attacks notwithstanding**,** it is difficult for hackers to trust each other completely due to the anonymous character of the online environment. Most hacking communities reside in what is often referred to as "The Deep Web", where hackers exchange knowledge, skills, and resources through forums and market, and use various tools to remain anonymous. There you can never be sure that the person you are talking to is not simultaneously working for the authorities or will hand you over to the authorities if sufficient proof of illegal activity is collected.[108]

The hacker community takes several steps to ensure a reasonable level of trust and quality of services offered on the black market. One particular system called the "escrow system" was set up in the early 2000s at the CarderPlanet black market. A third party officer was installed, who would mediate between the vendor and purchaser. The vendor, for instance, would offer stolen credit card details that the purchaser was interested in buying. The purchaser would then send the administrative officer a sum of digital money, after which the vendor would sell the stolen credit card details. The officer would then verify whether the stolen credit card worked, and, if so,

would pass the money to the vendor and the credit card details to the purchaser. Through this practice cybercrime in the Dark Web was revolutionized.[109] Fifteen years later, the third-party system is still commonly used in black markets.[110]

Another way is to limit the access to online hacking forums. It is through these forums that hacker groups are usually founded. Most forums can only be entered after a hacker has proven his or her skills, or has been invited by another member – thus limiting the chance of spying by the authorities. Forums often sort their activities on specific topics and practices, such as social media hacking, data theft, malware, exploits, hit-and-run attacks, etc.[111] Examples of hacking forums are EvilZone, HackHound, Bitshacking, Dark0de, and TheRealDeal.

Regular visitors who are active in a certain part of a forum are likely to get acquainted and slowly form a group. This group of friends then might expand by inviting other familiar hackers. Before starting an operation, the group will generally go underground, meeting up in private conversations and closed invite-only channels.[112] This method makes sense, since writing a forum-wide message might compromise the hackers´ operation (spies could inform the target or the authorities, which could solve the security vulnerability, or the actor who posted the message could be arrested). To minimize this risk hackers first organize themselves in a kind of inner circle, looking around forums, checking out who has which skills and who is considered trustworthy, and then inviting those they deem valuable (and reliable) for the new group.

However, sometimes a group that is (still) active in an "open forum", can become a major movement, containing hidden subgroups. An example thereof is Anonymous, which was originally formed in the 4Chan forum where "trolling" activities took place.[113] In 2008, the Anonymous movement started trolling actions against the Church of Scientology.[114] Anonymous launched a DDoS attack on the Scientology websites, combined with real-life actions such as ordering unpaid pizza's and escorts to Scientology churches, faxing images of nude body parts, etc. A short video made by a small group of participants ignited a serious debate within the rank and file of Anonymous. The video declared war on the Church with the result that individuals were spurred into debate and then catapulted onto the streets. Soon, over 7000 people in 127 cities protested the Church of Scientology's human rights abuses and censorships. With this, Anonymous shifted from coordinated trolling to being a political activist group. Over the next two years many joined the Anonymous movement setting up (unrelated) activist subgroups. Participants came to identify themselves as bona fide activists, often performing actions themselves.[115]

The mode of cooperation here is clear. Although Anonymous can be seen as representing a single movement, the structure of the organization is a constantly changing maze where multiple groups organize (and sometimes become quite powerful). Through private conversations and invite-only channels, the overall organization becomes highly complex and confusing. There is no central leadership. No single group or individual can claim legal ownership of the name Anonymous, as it is a classic anti-brand brand, assuming various configurations and meanings. Anonymous is composed of multiple competing groups. This structure makes short-term power achievable for brief durations, but long-term dominance by any single group or person virtually impossible. The sociology of Anonymous is thus a constantly changing labyrinth.[116]

This fluid and opaque organizational structure of many hacking communities also affects the nature of potential cooperation between hackers and NDOs. This kind of vertical cooperation between NDOs and hackers is the focus of the next Section.

3.3 COOPERATION BETWEEN NDOs AND HACKERS

Society's dependence on the smooth functioning of information systems has increased steadily. Cybercrime acts as an uncomfortable disruptor of this reliance. When disruptions to the critical infrastructure caused by a cyber-attack become so severe that they threaten the functioning of the state or, the act may be seen to transcend from the realm of crime into the realm of acts of war. Safeguarding the critical (information) infrastructure then becomes a matter of (national) defense. In trying to prevent or deter – e.g. through the ability to retaliate – these disruptive cybercriminal activities, can NDOs establish cooperation with hackers?

Before elaborating on the possibilities and (potential) benefits and risks of such cooperation, let us first look at some examples of the teaming up of NDOs and hackers in what, depending on the perspective, could be classified as either cybercrime or offensive cyber (as a military act). In its cyber strategy, the Dutch NDO has expressed the requirement for an offensive cyber capability, if anything as a means to retaliate and therefore to deter. In the context of "hybrid" threats and an integrated – equally hybrid – counter strategy, these examples may offer some interesting insights into how NDOs may leverage hacker communities for state purposes.

It should be noted that information on cooperation between NDOs and hackers is limited and, in many cases, classified. This lack of reliable information makes a comprehensive analysis virtually impossible. Yet, research done by computer security

firms, media organizations, and others provide many interesting details about recent high-profile cyber accidents, identifying a number of examples of recent cyber activities where cooperation between various NDOs and hackers is strongly suspected. These examples provide illustrations for a more general discussion of the benefits that NDOs can get by cooperating with hackers, as well as the challenges and risks that they are likely to encounter in the process of such cooperation.

3.3.1 CYBER ATTACK ON GEORGIA

In 2008, shortly before Russia's armed intervention in the Georgian province of South Ossetia, Georgian state computer servers were targeted by a series of cyber-attacks. The attacks against Georgia's Internet infrastructure started nearly a month before the conventional war, with a coordinated major DDoS attack that overloaded and effectively shut down Georgian servers.[117] Although there is no conclusive evidence that the attackers were Russian or acting on state orders, strong suspicions have come up. First of all, security researchers found that the HTTP-based botnet used on the command-and-control server was a MachBot controller, which is a tool that is frequently used by Russian bot herders. Second, the domain involved with the command-and-control server had false registration information but did tie back to Russia because the redirection of Internet traffic went through Russian telecommunications firms.[118] The software programs that controlled the attacks were located in hosting centers controlled by these firms. Some Russian-language websites, such as stopgeorgia.ru, also continued to operate and offer software for download used for DDoS attacks.[119]

However, even if Russian hackers were involved, this does not prove that the attack was also state sponsored. The attacks could be the result of Russia's IT-underground self-mobilization: hacktivists feeling obliged to send out a signal that they were actively participating in the political life and were monitoring events closely. Nationalistic articles in Russian newspapers could fuel tensions further and literally seek involvement of Russian hackers. This could ultimately become a self-fulfilling prophecy: by speculating about non-existent hacker discussions on coordinated attacks against a particular country, such discussions could actually start taking place.[120]

In the example of the cyber-attack against Georgia, it becomes clear that hackers can be an effective tool for instigating DDoS attacks. By mobilizing hackers and hacktivists, one can gain advantages in conventional warfare as DDoS attacks paralyze the opponents' country.

3.3.2 CHINA

In China, the People's Liberation Army (PLA) has also been connected to cyber-attacks on foreign countries. An example here is PLA Unit 61398, a group also known as Advanced Persistent Threat 1 (APT1), Byzantine Candor, or The Comment Group. This last name was derived from the group's trademark of infiltrating computers using hidden webpage computer code known as "comments".[121]

From 2010 until 2012, the group worked each day from nine to five Beijing time, transferring the crown jewels of US corporations' proprietary data out of their networks – and into computers in China.[122] Although Google already reported a hack into their network back in 2010, the group only became publicly known in 2012 after hacking into the e-mails of the president of the European Union Council, Herman van Rompuy.[123] The breach likely enabled the intruders to obtain an insider view into the financial crisis gripping Europe.

However, the hackers themselves were also being hacked. Working together in secret, 30 North American private security researchers (under the leadership of internet security firm Mandiant) exploited a hole in the hackers' security. The researchers created a digital diary, logging the intruders' every move as they crept into networks, shut off anti-virus systems, camouflaged themselves as system administrators, and covered their tracks, making them almost immune to detection by their victims.[124] These minute-by-minute accounts showed a highly organized effort from a group with fixed routines and high success rates. Soon thereafter, the group was linked to the Chinese military, since many of the organizations targeted lost information that could help China in its attempts to become the world's largest economy. The targets included lawyers pursuing trade claims against the country's exporters and an energy company preparing to drill in waters China claims as its own.[125]

The Chinese government denied official involvement, stating that the activity was the work of rogues[126] and that the research would rely only on linking tracked IP-addresses.[127] However, certain parts of the evidence cited by experts suggest that the hacking was in fact state-sponsored. Most convincing was the fact that none of the work was done in the weekend but coincided with Beijing standard working hours. This does not match with the idea of mere hobbyists or hacktivists. Also, the persistence of the attacks was typical for Chinese hackers and the information stolen was mostly about pricing, manufacturing, corporate acquisitions, and contract negotiations.[128]

In this example, another form of cooperation between NDOs and hackers is evident: using hackers through fixed employment. The benefit of this form of cooperation is that it ensures control over hackers' activities and significantly increases coordination of their actions (which in turn increases the success rate). At the same time, the NDOs ability to plausibly deny its involvement, although diminished, remains.

3.3.3 STUXNET

In 2010, a computer worm known as "Stuxnet" targeted industrial and factory systems. Stuxnet was extraordinary – not only because it was, as Alan Bentley, senior international vice president at security firm Lumension has stated, "the most refined piece of malware ever discovered," but also because "mischief or financial reward was not its purpose – it was instead aimed at the heart of critical infrastructure."[129] The Stuxnet worm became famous after it sabotaged the centrifuges used to enrich uranium gas in the Natanz uranium enrichment plant in Iran. Stuxnet was unlike anything ever seen before: it did not hijack computers or steal information from them, but instead destructed the equipment of the controlled computers by placing malicious files on one of the systems. Soon the worm became known as the world's first digital weapon.[130]

Naturally, the question of who was behind the Stuxnet attacks was quickly posed. Security experts who investigated the worm stated that it was almost certainly the work of a national government agency but also warned that it would be near-impossible to identify the culprit.[131] However, strong suspicions have come up that the US and Israeli governments were involved, as they would have had much to gain from a slowdown of Iran's apparent progress towards building an atomic bomb without launching a traditional military attack.[132] According to anonymous US officials speaking to the Washington Post, the worm was indeed developed in cooperation with the Israelis during the administration of George W. Bush. The aim was to sabotage Iran's nuclear program with what would seem to be a long series of unfortunate accidents. The malware was supposed to make the Iranians think that their engineers were incapable of running an enrichment facility.[133] The cyber weapon in this case served clear political motives, namely preventing Iran from acquiring the ability to make nuclear weapons.

The examples described above show the difficulties in determining who was responsible for an attack and whether it was implicitly or explicitly state-backed. Cyberspace is essentially a borderless space where the physical location of an individual does not significantly affect his or her capacity to carry out a cyber-attack.

The internet provides numerous options to hide or to conceal its user's true identity. This makes attribution of a cyber-attack a difficult, and, in some cases, nearly impossible task. Uncertainty and plausible deniability regarding cyber activities make them well suitable for covert operations.

3.4 BENEFITS OF COOPERATION

The examples described in the previous Sections all required at least some degree of either white hat or black hat hacker participation. Cooperation between NDOs and white hat hackers is not a new phenomenon. The Dutch NDO has since late 2013 been actively working on recruiting white hat hackers as so-called "cyber reservists". These hackers are requested to take part in basic military training a few times per year and accompany missions as a cyber security expert, when so required.[134] On top of the reservists program, the Dutch MOD's Cyber Command has, in collaboration with IT security firm Fox-IT, jointly trained defense employees to become cyber security specialists. The first 14 graduates finished their education in May 2015 and were subsequently stationed with the Dutch Cyber Command, the Military Intelligence Service, the Defense Computer Emergency Response Team (DefCERT), and with the Royal Netherlands' Marechaussee.[135]

The novelty factor lies in cooperation with black hat hackers. But why would NDOs consider cooperating with black hat hackers in the first place? One reason could be a superior skillset. Compared to white hat hackers, black hat hackers tend to be more skilled, better trained, and more up to date with the latest security exploits and countermeasures. Black hat hackers will focus only on security penetration and will thus have more security knowledge than other IT professionals.[136] As a result, they are likely better placed to counter other black hat hackers. Therefore, hiring black hatters to test defenses of an organization against cyber-attacks is possibly an attractive idea. Their real world hacking experience is a distinct advantage for security penetration testing.[137] Furthermore, black hat hackers are better equipped to act on the verge, and possibly over the edge, of legality compared to white hat hackers. However, at this stage Western MODs are not, at least not openly, willing to pursue this route.

As Brien Posey, a former gray hat and now white hat hacker and co-owner of a security research firm points out: "There are some things that you just can't learn from a book. (...) Every hack is different because every network is different. (...) Often hackers have to combine multiple techniques or apply techniques in a different way than normal to compensate for various network defenses. Only someone with plenty of real world hacking experience can efficiently go from using one technique to another as required by the present situation".[138]

3.5 RISKS AND CHALLENGES

Successful cooperation between NDOs and hackers is hindered by significant barriers. First, hackers must be identified. Second, they must be convinced to cooperate with a NDO. Third, their work must be coordinated and monitored. Resolving all these problems successfully is not easy. Liberal democracies face additional legal, ethical, and other constraints and barriers in their dealing with hackers. Below we consider these issues in more detail.

3.5.1 IDENTIFICATION

The first problem is to identify hackers with whom a NDO might be interested in cooperating with. As almost any sizeable organization knows, this is not a simple problem even when all conventional recruiting tools (job advertisements, job fairs, recruiting presentations, etc.) are available. These conventional tools can be used in identifying and attracting some hackers, in particular white and gray hats. Hackathons and hacker conferences offer one attractive option for such a recruiting effort. The US government has made notable efforts recruit hackers in this way. In 2011, the US government launched a massive recruiting effort to hire experienced computer employees, who can help defend the nation in cyberspace. To do so, officials from the Department of Defense, the Department of Homeland Security, and the National Security Agency mingled with the 10,000 visitors of DefCon, the world's largest hacker conference.[139] The recruitment effort has been called this generation's "Manhattan Project": the government has set up camps and held cyber competitions for teenagers and has offered scholarships, internships, and jobs in cybersecurity to young adults. With this, the severe shortage of cybersecurity experts working for the federal government should be eased.[140] As the Netherlands also has a shortage of cybersecurity experts, the Dutch NDOs' efforts to recruit cyber reservists and actively train defense employees to become cyber security officials is a logical development.[141] These kinds of efforts are likely to have only limited success in identifying and recruiting skillful black hat hackers. These individuals have strong reasons to hide their real identities and use anonymity that the Deep Web can still provide. So what more can NDOs do to identify black hat hackers? They could choose to infiltrate a hacker community. To do so, a NDO would have to hire an identified hacker and place him or her as a mole in the community. Hiring this one hacker could lead to a snowball effect, as he or she will give away others, who are subsequently incentivized to rat out more hackers to avoid criminal charges. This in turn weakens the entire community structure: it will be difficult for individuals to find each other and forming groups will be particularly cumbersome as there is an increased likelihood that someone in the group is an informer.

Kevin Poulsen, senior editor at *Wired* magazine underlines this view by pointing to the hacker collective's classical vulnerability to infiltration and disruption: "[w]e have already begun to see Anonymous members attack each other and out each other's IP addresses. That's the first step towards being susceptible to the FBI."[142] Conversely, hackers are increasingly aware of this tactic. Barrett Brown, who has acted as a spokesman for the otherwise secretive Anonymous says: "[t]he FBI are always there. They are always watching, always in the chatrooms. You don't know who is an informant and who isn't, and to that extent you are vulnerable."[143]

3.5.2 COOPERATION

After a NDO has identified individuals that it would want to involve in its activities, whether on a regular basis or in an on-call manner, its next step is to persuade those individuals to cooperate. According to Alexander Klimburg, author of "Mobilising Cyber Power", governments have three ways of ensuring a hackers cooperation: coercion, cooption, or convincing.

Coercion assumes involuntary cooperation via the use of negative incentives (sticks), such as pressure, intimidation and force – or threats to use these techniques. Coercion can be used to compel hackers to cooperate who have been caught by offering them reduced sentences or dropping criminal charges against them in exchange for cooperation. This kind of cooperation probably more often takes place as on-call engagements rather than as full time employment. An example here is the case of Hector Xavier Monsegur, or "Sabu" as this celebrated hacker was known online. Monsegur is one of the hacker world's most hated figures, as he turned from being the leading figure in the Anonymous and LulzSec collectives into what was (in effect) an undercover FBI agent. The skilled hacker was facing a maximum sentence of 26 years according to official guidelines but as a reward for having spent much of three years working as a federal informant, was eventually sentenced to time served (equivalent to the seven months he already spent in prison plus one year's supervised release).[144]

According to Eric Corley, a well-known hacker and publisher of the hacker quarterly 2600, Monsegur is not the only US-agent in the hacker community. In an article by the Guardian, he states that one in four US hackers is an FBI-informer, making the US hacker community thoroughly infiltrated. Cyber policing units have successfully forced online criminals to cooperate with investigations by threatening them with long prison sentences. "Owing to the harsh penalties involved and the relative inexperience with the law that many hackers have, they are rather susceptible to intimidation," says Corley.[145]

Russia and China are also likely to use coercion to force cooperation from hackers, but information about such cases does not become public often. In one example from Russia, a suspected cybercriminal appeared in government advisory positions and worked closely with Russian security agencies.[146]

Cooption is another way to promote cooperation with hackers. Cooption is about implied rewards provided through political structures designed to support the political elite. Russia supposedly uses cooption in its cybersecurity strategy. An example here was the Putin-aligned youth group "Nashi", which was implicated in the 2007 cyber-attacks that paralyzed Estonia.[147] Another example is the ATP28 group, which was recently investigated by the cybersecurity company FireEye. According to their report, ATP28's work is sponsored by the Russian government. Not only has the group targeted inside information from governments, militaries, and security organizations that would benefit the Russian government, but the group has also used malware that is developed using Russian language settings during working hours consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg.[148]

In China, cooption is also used by the Chinese government to induce cooperation from hackers. This is, first of all, done through a system called the "National Defense Reserve Forces" program. Through this system, each student enrolled in a technical study automatically becomes part of the Chinese Defense Organization. Furthermore, China's People's Liberation Army (PLA) organizes hacker competitions, through which they identify talented hackers – and subsequently keep them safely occupied. Though the official statement of the Chinese Government is that this cyberwarfare strategy is purely defensive, suspicions have risen that China is operating offensively as well. Governments, companies, and internet security experts around the world have blamed China for many of the past year's global hacking attacks.[149]

The result of China's policy is clear: the country has acquired a strong cyber force, which can – even though China denies it – be deployed both defensively and offensively. However, as Klimburg points out, the bulk of Chinese cyber activity seems to be directed at internal control, either directly (through propaganda, censorship, and collusion) or indirectly (through schemes designed to bind and coopt potentially dangerous individuals, particularly patriot hackers). As with traditional informer systems found in most authoritarian states, the real targets of this system are not the people being spied upon (or, in cyberspace, being attacked). The targets are rather the spies themselves, who are thus coopted by the state and become less likely to turn against the regime.[150]

Convincing is probably the preferred method for a NDO. This means that hackers will voluntarily engage in activities that a NDO would want them to do. In the case of the massive DDoS attacks on Estonia in 2007 and Georgia in 2008 there are reasonable grounds to believe that some participants were motivated by broader national interest (as they saw them) rather than by coercion or cooption. The problem with this particular way of working is that it is fluid and uncertain, and therefore hard to manage. It is difficult to be sure that it can be mobilized at a particular moment in time and at a desired scale.

3.5.3 COORDINATION

Finally, once hackers are identified and convinced, through one way or another, to cooperate, there is the challenge of coordinating and monitoring their cooperation. One particular problem in employing hackers within a NDO is the issue of trust. By definition, black and grey hat hackers would not pass a conventional background check. Can a black hat hacker actually be trusted? How can one be sure that a hacker is not selling a vulnerability he uncovered on the black market, or even worse, inserts a new vulnerability? In other words, how do you make sure that the hired hacker will not become a Trojan Horse? Related to this is the issue that hackers could turn out to be double agents. When the hired hacker finds a vulnerability in a system, he or she could first sell this knowledge on the black market, and only report the leak afterwards. That way, the hacker will receive money twice: once from the seller on the black market and once from the NDO who hired them. Also, in a broader sense, as the hacker will receive knowledge of the systems security, he or she could leak (classified) NDO documents.

In general, taking hackers into your organization is a risky business. Nevertheless, some companies have had successful experiences in hiring black hat hackers. For instance, in 2011 Facebook hired George Hotz, online known as "GeoHot". Hotz unlocked both Apple's iPhone and Sony's PlayStation game consoles and posted details of how to alter software on the devices. This way, crafty tech users could use them for unauthorized games and other applications. Sony, furious with this, publicly sued Hotz on eight claims, including violation of the Digital Millennium Copyright Act, computer fraud, and copyright infringement. After a nasty legal battle of three months, Sony and Hotz reached a settlement. As part of this settlement, Hotz agreed to wipe all PS3 hacking resources from the web. Only a few days after the settlement was made public, Hotz was employed by Facebook, where he was reported to be working on building an anti-hacker defense program.[151] In 2014, Hotz left Facebook to start working for Google, where he joined Google's vulnerability research team Project Zero.[152]

Another example is the case of Nicolas Allegra, pseudonym "Comex", who was hired by Apple in 2011 – only two months after creating the JailbreakMe hacking tools for iPhone and iPad. After one year, Allegra left Apple to start an internship at Google.[153] Allegra was not the first hacker to be hired after successfully hacking iPhones and iPads. In 2009, then 21-year old Australian Ashley Towns created the first known iPhone worm, which set a photo of singer Rick Astley as a mobile wallpaper. Towns was quickly hired by Mogeneration, an iPhone app developer based in Sydney, Australia.[154]

A final example is Michael "Mikeyy" Mooney, who in 2009 (at the age of 17) coded a Twitter worm sending tweets from hundreds of accounts. In an interview with ABC News, Mikeyy said he received several job offers after the attack. The one he accepted was as a developer for Oregon-based web application developer exqSoft Solutions.[155]

In hiring hackers, NDOs should keep in mind that they are not your average employee. Hackers conform to a distinctive subculture, which could result in substantial cultural differences between them and the existing NDO culture. Limiting a hacker's freedom is a general no-go: as soon as a hacker feels restricted, he or she will probably walk away.[156]

Security clearance requirements are likely to be another barrier for hiring hackers. Weed smoking longhairs or hackers with a criminal record cannot possibly obtain the necessary clearances, which limits NDOs in hiring the best hackers out there. To employ truly talented hackers, NDOs will therefore have to broaden the scope of their hiring criteria and focus more precisely on an individual's hacker skills.[157]

3.6 MODELS OF COOPERATION

The problem of how NDOs in liberal democracies could cooperate with hackers is a complex one and involves many legal, ethical, technical, societal, and management issues, which differ from country to country. There are many different ways of organizing and coordinating such cooperation. Applegate proposes four models for incorporating "patriotic hackers" and civilian technicians into militia-like structures and integrating these types of organizations into a state's cyber operations (see Table 4).[158]

MODEL	LEGALLY PART OF NDO?	MEMBER[I]	BENEFITS	DRAWBACKS	COST
FORUM	no	P / A	• Pool of skilled/diverse technicians • No requirements to military standards	• Limited to non-combative activities • Difficult to enforce ethical constraints • Little control • Information leakage	< €
PUBLIC / PRIVATE CELL	no (in most cases)	P	• Higher security level • Difficult to infiltrate • Flexible in duration • Specific skillsets	• Traditional contracting practices • Vetting required	€
REGULAR RESERVE	yes	P	• Well trained experts • Formal induction into military • Fast mobilization	• Active duty standards • Little incentive for formal induction • Formal training requirements	€ € €
CYBER READY RESERVE	yes	ex-P	• Highly qualified technical professionals • Quick mobilization • Legal combatant status • Traditional ethical, legal, and operational constraints • No formal training	• Difficulty of organizational integration • Little understanding of the mission • Difficult to match experts and place • Little skill validation or maintenance	€ €

TABLE 4: FOUR MODELS FOR DEFENSE-HACKER COOPERATION. SOURCE: APPLEGATE, 2012.

P= PROFESSIONAL. A= AMATEUR.[159]

The first of Applegate's models – the forum – uses formalized forums for limited cyber operations. The membership is primarily composed of security professionals, security researchers, and technicians. States could use these forums for open source research, code review, and as a recruiting pool for selected projects. While inexpensiveness and no requirements of military standards on appearance or physical fitness make this model lucrative, it is also difficult to enforce ethical constraints or control actions of

individual forum members. More importantly, there is a risk of information leakage: it would be easy for a competitor state to infiltrate this type of organization.[160] An example of a forum model is the network of Warning, Advice and Reporting Points (WARPs) in the UK. A WARP is a forum of 20 to 100 members created to provide warnings about possible cyber incidents to its members – either local governments, legal organizations, or businesses. At the head of a WARP, there is an operator who distributes the information among the members.[161]

The public/private cell model puts together a small group of hackers who most likely know each other in a group or cell. This composition is more secure, more difficult to infiltrate and would also make use of members´ specific skill sets. On the other hand, traditional contracting practices would probably be required, and members' background would also need to be examined.[162] Two examples of hacker cells are "Team Evil" and "Team Hell", even though these are not known to have cooperated with defense.[163] Team Evil, an anti-Israeli hacker group, was predominantly active in 2006 when it attacked over 8,000 websites of Israel and other countries, such as Saudi Arabia, China, and Indonesia. Team Hell is a secular Saudi hacker group which has shown aversion to the Israeli and Syrian regimes and al-Nusra, for instance.[164]

Applegate proposes two other models for cooperation between NDOs and civil technicians or ICT experts – the regular reserves model and the cyber ready reserves model. The former encompasses employing active duty military personnel in cyber operations and the latter recruits "cyber soldiers" – professional soldiers that have finished their military service obligation.[165] These models essentially focus on building cyber security capabilities within NDOs through education and training. Neither model, however, directly touches upon the nature of the cooperation between the defense forces and hackers and as such are not discussed in more detail here.

3.7 APPLICABILITY FOR NDOs

It is evident that cyber space is becoming more and more important for NDOs. Both defensive and offensive cyber capabilities need to be strengthened. The use of skilled hackers might well form part of this capability build-up. Hackers have better knowledge and skills of how to gain entry into a system then classically educated and operating IT professionals, since they have real world hacking experience. On the downside, we see two principal disadvantages or risks in employing hackers as part of the cyber capabilities of NDOs:

- *Trust*: it remains difficult to know whether a hacker is truly working for you. Because of their unique skills and the difficulty to monitor their work, hackers might become double agents, revealing critical vulnerabilities to criminal organizations or other countries.
- *Culture*: there are fundamental differences between the hacker culture and the typical military culture that may create severe tensions.

In working with hackers, there is a crucial difference between so-called white hats and black hats. In many respects, employing or hiring white hat hackers seems not very different from engaging other types of specialists. There might be an issue of whether governments can afford to employ the capable ones, but that is no different than, say, for other scarce categories. This is a route already taken by the Dutch MOD. It is too early of a stage to assess whether it is a successful route, but it seems likely that any obstacles along the way would rather point toward other solutions to negotiate the route instead of choosing to abandon it altogether.

Engaging with black hat hackers is a completely different story. It would be a principled choice to engage with black hats at all, considering the political, judicial, and ethical liabilities. For manty western NDOs, the will and authorization to do so in a structural way seems unlikely. And even then, a host of practical questions and difficulties arise. These principal and practical issues must be set against the anticipated benefits. Reasons for using black hats may, for instance, be that they are better skilled, more versatile, and more up to date with the latest security exploits than white hats; have a much wider range of options beyond what government agencies may do; and that they are better placed to counter other black hats (it takes a thief to catch a thief). In our (limited) analysis, apart from some anecdotal snippets, we have not been able to come up with conclusive facts and figures to either substantiate or dismiss these propositions.

An intermediate solution would be to employ black hats turned white. However, it might be that many of the potential advantages of using black hat hackers quickly disappear once they are brought within the operational and legal framework associated with white hat hacker activities.

There is, however, another angle for taking a closer look at how hacker communities operate from a NDOs' perspective. The hacker community operates on, and often beyond, the brink of legality. In the twilight zone of the dark web, relationships are

forged. Because of their clandestine nature, these relationships are either very exclusive or fleeting, often lacking a basis of trust, and therefore as a rule uneasy, if occasionally very rewarding for the participants. In contrast, NDOs typically enter into long-term relationships with trusted partners, based on formal agreements and well-understood, stable mutual interests. However, there is a distinct trend for NDOs to engage not only in long-standing, high-trust partnerships, but also in more ad hoc, informal, and even implicit forms of cooperation with unfamiliar parties, and even with parties considered untrustworthy or outright hostile. The complexity of the security environment increasingly demands willy-nilly interactions with actors one would rather not engage with, but that within a given situation may be instrumental in achieving certain desired political or strategic effects. Some of these interactions may indeed resemble the way in which hackers engage one another. It is this realization that makes this case interesting: what may NDOs learn from methods the hacker community employs to create goal-oriented working relationships between agents that do not really know each other, do not trust each other (or even actively distrust one another), and might even have contradicting values and interests outside the scope of a limited and temporary alignment?

Within the scope of this study, we did not elaborate much on this particular angle. But it certainly seems an interesting notion to pursue further elsewhere.

3.8 PRACTICAL EXAMPLES

China and Russia can more readily coerce, coopt, and convince hackers than most Western democracies – although a large portion of their cyber activity is directed at internal control rather than on external use.

One of the more recent cases where Russia's offensive cyber power became apparent is in Ukraine. Ukraine has been faced with a separatist conflict in its east for two years now, during which the Russian government has been suspected of instigating numerous cyber-attacks. For instance, BlackEnergy, a Russian malware, was used in the summer of 2014 against the Ukrainian government by a hacker group called Quedagh.[166] In October of that same year hackers, most probably Russian, attacked several computers of international organizations, companies (for example energy companies), and the Ukrainian government. The attacks are believed to be part of a years-long operation of Russian hackers due to the code language and the targets involved.[167] In late February and early March 2014, telecommunication company Ukrtelecom came under attack. The vast majority of regional services provided in Crimea were soon out of order.[168] The attack also influenced the mobile phones of

Ukrainian politicians, which were blocked by malicious software.[169] While it is not confirmed who was behind the attack, it is believed that the unknown hacker or group of hackers were affiliated with the Russian government, with the aim of isolating Crimea from Ukraine. It is suspected that the Russian vessels that arrived in Sevastopol contained jamming tools and hence were placed there in order to hinder radio transmission.[170] Around the same time, other Ukrainian actors faced cyber-attacks, such as the UNIAN news agency and the journals Glavnoe and Gordon. The Ukrainian government, Verkhovna Rada, and the Ukrainian Security Service also faced DDoS attacks.[171]

China's use of offensive cyber capabilities is illustrated by the example of one man, Tan Dalin, which is described in a document posted by the Obama Administration.[172] As a student, Dalin was invited to participate in a People's Liberation Army (PLA)-sponsored hacking contest. When he won, he formed the group "Network Crack Program Hacker" (NCPH) and recruited other talented hackers from his school. He managed to find a funding source (unknown benefactor) and started attacking US sites. After an initial round of successful attacks, his funding was tripled. Throughout 2006, NCPH built sophisticated rootkits and launched a barrage of attacks against multiple US government agencies. By late July 2006, NCPH had created around 35 different attack variants for one MS Office vulnerability. During the testing phase, NCPH used Word document vulnerabilities. Later, they switched to Excel and PowerPoint vulnerabilities. The result of all of this activity is that the NCPH group siphoned thousands, if not millions, of unclassified US government documents back to China.[173]

What these groups consist of and how they work is mentioned in Kathrin Hille's work "Chinese Military Mobilises Cybermilitias": "[These groups comprise] 25-year-olds or 17-year-olds [who] have 40-year-old fathers who happen to be working within institutions. Very often the opportunistic exploitation of a particular low-tech approach is derived through that chain, completely informally, rather than through somebody sitting in committee and deciding let's build 500 botnets that we're going to use to attack the Tibetan community."[174]

It is not a given that Western NDOs can go down similar routes. The problem of how NDOs in liberal democracies should cooperate with hackers is a complex one and involves many legal, ethical, technical, societal and management issues, which differ from country to country. Applegate proposes four models for incorporating patriotic hackers and civilian technicians into militia-like structures and integrating these types

of organizations into a state's cyber operations (see Table 5). Two of these four models are non-traditional in nature. The forum model uses formalized forums for limited cyber operations. The membership is primarily composed of security professionals, security researchers, and technicians. States could use these forums for open source research, code review, and as a recruiting pool for selected projects. While inexpensiveness and no requirements of military standards on appearance or physical fitness make this model lucrative, it is also difficult to enforce ethical constraints or control actions of individual forum members. More importantly, there is a risk of information leakage: it would be easy for a competitor state to infiltrate this type of organization.[175] An example of a forum model is the network of Warning, Advice and Reporting Points (WARPs) in the UK. A WARP is a forum of 20 to 100 members created to provide warning about possible cyber incidents to its members – either local governments, legal organizations, or businesses. At the head of a WARP, there is an operator who distributes the information among the members.[176]

The second non-traditional model is the public/private cell model, which puts together a small group of hackers who most likely know each other in a group or cell. This composition is more secure, more difficult to infiltrate and would also make use of members´ specific skill sets. On the other hand, traditional contracting practices would probably be required, and members' background would also need to be examined.[177] Two examples of hacker cells are Team Evil and Team Hell, even though these are not known to have cooperated with defense.[178] Team Evil, an anti-Israeli hacker group, was predominantly active in 2006 when it attacked over 8,000 websites of Israel and other countries, such as Saudi Arabia, China, and Indonesia. Team Hell is a secular Saudi hacker group which has shown aversion to the Israeli and Syrian regimes and al-Nusra, for instance.[179]

4 CASE STUDY 3 – ‘USHAHIDI, AN OPEN PLATFORM FOR SITUATION AWARENESS’

4.1 USHAHIDI HAITI PROJECT 80
4.2 BENEFITS OF USING USHAHIDI 85
4.3 DRAWBACKS OF USING USHAHIDI 88
4.4 IMPROVEMENTS 91
4.5 APPLICABILITY FOR NDOs 93
4.6 PRACTICAL EXAMPLES 96

4 CASE STUDY 3 – 'USHAHIDI, AN OPEN PLATFORM FOR SITUATION AWARENESS'

By their very nature, humanitarian relief operations (HROs) involve a wide range of actors who need to obtain and process large amounts of information in a short period of time and in a coordinated fashion. They then also need to make this information actionable and actioned. This makes HROs a worthwhile area to investigate new forms of cooperation. Since every single operation is in a way unique, there is not only the issue of cooperation but also the need for actors to be adaptable and to be able to reconfigure cooperation mechanisms as the needs and circumstances change. We submit that this, too, makes them interesting cases studies for NDOs who are grappling with new ways to cooperate with new partners.

Rapid advances in communications technology have enabled responders to global disasters to operate in much more effective ways. This is not only the case for small and nimble organizations, but also for larger, more traditional actors, such as government agencies. The need for better means to coordinate and monitor operations arose in particular in the wake of the 2004 Tsunami in East Asia. Since then, new platforms have been developed, some of which have proven quite successful and have been replicated elsewhere. One such example is Ushahidi.

Ushahidi is both a website and non-profit company that developed an open source crisis map out of the need to provide alternative information about incidents of violence in the post-electoral period in 2007 in Kenya. At the time, the Kenyan government established a ban on free media coverage and reserved the right to review all articles and reports that were broadcasted and published. As a result, there was a scarcity of reliable information. This prompted Ory Okolloh, a blogger and activist, to use her blog to collect information about eruptions of violence. As she received a vast amount of reports and realized that a blog alone is an inadequate tool, she decided to create a website where people could share information that was banned by the government. With the help of several developers, Ushahidi was up and

running the same week.[180] It was an online map that showed instances of violence in Kenya. Moreover, as a truly open platform, Ushahidi enabled anyone who wished to share information to report and contribute to the map. Since then, Ushahidi has been deployed in a number of humanitarian crises, including the 2013 Japanese tsunami and the 2010 Haiti earthquake, and is also used for other purposes in Congo, Mexico, and the US.[181] It has been used to support various humanitarian responders such as the US military, the United Nations, and a number of non-governmental organizations.[182] Ushahidi's chief contribution to HROs is to make geospatial data available by consulting sources that the relief community had not exploited – ranging from digitized data to weather forecasts. For this process, geospatial technologies combining geographical data (such as GPS location) and spatial software (such as Google Earth) are required. Geospatial data, however, is not new to traditional humanitarian actors. And while geospatial technologies have high potential for crisis management, many countries or whole regions run into the difficulty of either not possessing the means of geospatial data collection or of the inability to establish proper geospatial services despite the data being available.[183] In such cases, Ushahidi or other crisis mapping platforms can fill the gap. These platforms use data available from local communities –through gathering text messages, online reports, or social media posts – and convert this raw data into a readily available crisis map constructed by a body of international volunteers.

4.1 USHAHIDI HAITI PROJECT

When Haiti was struck by an earthquake in 2010, the traditional humanitarian relief system was not functioning effectively. Humanitarian relief operations relied on the closed and rigorously structured network of relief workers and organizations. They heavily depended on the UN cluster in performing their duties. This was partly due to the belief among the organizations involved that experts with years of experience and the required skills could provide more accurate data of the situation on the ground and were thus more effective in providing disaster relief. In the wake of the Haitian earthquake, it became clear that this traditional approach fell short as a result of the inability to use new technological inventions and to explore new sources of information.[184]

In the past decades, the online environment has evolved to such an extent that an approach that does not respond and adapt to a changing social environment will have problems surviving. Making use of new technologies and opportunities, Ushahidi was a revolutionary and a paradigm-shifting development in the field of humanitarian aid.[185] However, the revolutionary approach of Ushahidi was not determined only by new

technologies; the technology that was used, such as text messages or the internet, had been there for some time already. The difference is made by the involvement of local residents and by using their knowledge in operational decisions.[186] This can be seen as the primary lesson learned from responding to the Haiti earthquake.[187]

There were other, Haiti-specific reasons for the need to engage Ushahidi and like-minded platforms after the earthquake. First, relief workers in Haiti were occasionally kidnapped, which resulted in the deterioration of communication between local leaders and the relief community.[188] Second, a proper backup of Haitian geodata did not exist, which proved to be an issue after the crisis and after the collapse of Haitian infrastructure. A freely available online map of Haiti was also not fully developed, and as a result it was a challenge and a task for international volunteers to help map the island's geography and infrastructure. Third, although the island asked for help from international volunteers – and indeed received help from various countries, foreign ministries, militaries, and (relief) organizations – local knowledge of the Haitian community stayed underexplored.[189] At the time, the relief community did not sufficiently recognize the opportunity of using open source maps to respond to crises, due to the rather novel nature of the application.[190] The widespread use of mobile phones, which boomed after 2006 when Digicel was introduced to the Haitian telecommunication market, acted as a key-enabler of the use of this type of technology.[191]

The open nature of Ushahidi is, according to David Kobia, a co-founder of Ushahidi, the main distinguishing characteristic of the new approach. He explains that the traditional approach uses a "one-to-many relation" with unidirectional flows of information. For instance, the Red Cross, an organization with many field presences, would be the source of information for stakeholders involved. Now Ushahidi collects data from numerous sources and establishes a relation where many (volunteers) help many (members of the affected community).[192] Therefore the idea behind the initiative is that the potential of a dataset of many sources outweighs that of information coming from a single source of information. The Ushahidi Haiti project collected thousands of text messages sent to an emergency reporting system that were first translated and subsequently categorized and geotagged by a team of volunteers. The information was then sent to humanitarian responders. Through this crowdsourced initiative Ushahidi was able to provide near-live and dynamic maps with information such as food requests and affected locations, which in turn facilitated relief efforts (see Figure 6).

FIGURE 6: FOOD REQUESTS PUBLISHED ON USHAHIDI HAITI WEBSITE. SOURCE: GAO, BARBIER, AND GOOLSBY, 2011.[193]

Figure 6 illustrates food requests on Ushahidi Haiti based on the number of reports mapped on Ushahidi's crisis map. Using these maps, relief organizations could coordinate resource distribution and make better decisions based on their analysis of crowdsourced data.[194]

Booker calls the strategy employed by Ushahidi a "wiki approach": it makes use of the internet's collaborative environment and creates a database of shared knowledge. He emphasizes the idea of a collective – actions are undertaken collectively and knowledge, too, is produced collectively. Ushahidi's wiki lies in the assembly of volunteers who not only come together as a joint force and perform a "collective action", but they are also involved in creating and developing the product itself, hence "peer production."[195]

An early Ushahidi Haiti version was up and running within an hour after the earthquake had struck through a joint effort of Patrick Meier, Ushahidi's core team member, and David Kobia, Ushahidi's tech development director. Meier, pursuing his doctorate at the Tufts University, convinced several students at Tufts to join the effort and this team later became the core of the whole project. At the same time, another initiative had come together to secure a free text messaging service. Individuals from FrontlineSMS:Medic, Digicel, and the US State Department got in touch through social media and email and managed to secure an already existing number, 4636, that previously collected information about the weather. The team got permission from the owners to use it for humanitarian purposes.[196] Ushahidi was one of the initiatives that had access to the messages sent to the 4636 shortcode.

Ushahidi Haiti was a truly cooperative and open initiative, both internally and externally. It relied on a body of volunteers who took care of the mapping, giving an equal chance to anyone with the basic skills and tools needed to perform the job. Many of these volunteers came from the Haitian diaspora[197] in the US, especially from Boston, where Ushahidi Haiti set up its headquarters.[198] When it comes to the external environment, the cooperative nature of Ushahidi Haiti was reflected in the very function of the whole project; it simply could not have been successful without cooperating with other partners. Despite the amount of work done by volunteers and the core team, the bulk of the essential tasks (e.g., translation, analysis, and tracking) were not provided by Ushahidi itself.

As a project that relied substantially on the work of volunteers, Ushahidi Haiti's internal structure was open to anyone. Any individual could join the project and contribute their skills and enthusiasm without having to sign a contract or otherwise commit themselves for a particular time period. They could, therefore, end their involvement in the project at any time. The open structure translates into a low systematic coordination of volunteers and is characteristic of open source platforms in general. This contrasts markedly with traditional crisis management systems which focus heavily on promoting standardized procedures and protocols that would effectively coordinate all efforts by governments, non-governmental organizations, and other relief workers.[199]

There was some effort to coordinate Ushahidi Haiti's volunteers, albeit small. As Ushahidi Haiti was a new platform and many of the recruited volunteers were unfamiliar with how it worked, it was difficult for some of those involved to contribute without proper instructions and support. Ushahidi thus served as an online support platform where its volunteers, the people involved in other initiatives, and the Haitian population could interact.[200] Ushahidi Haiti's volunteers also served as an intermediary between the Haitians and the relief community at large. Gao et al. introduced the idea of a crowdsourcing platform as an "interagency map" (see Figure 7), which connects relief organizations and the public through establishing relationships with both.

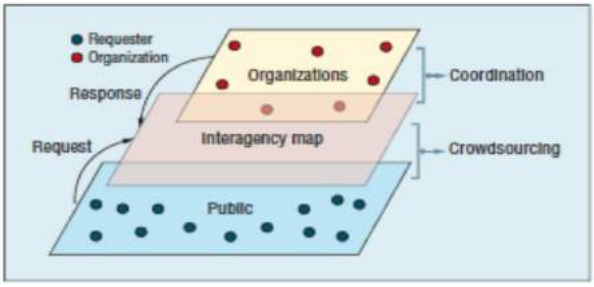

FIGURE 7: INTERAGENCY MAP. SOURCE: GAO, BARBIER, AND GOOLSBY, 2011.[201]

The Haitians provided information by sending aid requests through messaging service or the internet. The data was then crowdsourced by volunteers of Ushahidi and other projects and provided to relief organizations who could then respond to specific requests. The interagency map also serves as a tool for the organizations to "collaborate, plan, and execute shared missions," based on the information provided.[202]

However, after the Haitian earthquake, there were numerous crowdsourcing initiatives that served as an interagency map. In such cases, coordination of these projects would be beneficial to the whole humanitarian operation. But beyond the exchange of information with other projects, there was little integration of Ushahidi with other crowdsourcing initiatives, also owing to some disagreements between these platforms.[203] That said, the benefits of crowdsourcing in complex theaters that suffer from unrest as a result of (natural) disasters is increasingly recognized for use in different operational settings (see Figure 8).

GAMING AS A STRATEGY DEVELOPMENT TOOL

The benefits of crowdsourcing in coming to grips with zones that experience high levels of turmoil, whether as a result of disasters or conflict has also been recognized in an initiative of the US Navy called the *Massive Multiplayer Online Wargame Leveraging the Internet*. This is an online game that analyzes the moves of players. The information this game yields serves as a tool to explore possible warfare scenarios and new strategies and has been used for instance against piracy in Somalia.

FIGURE 8: GAMING AS A STRATEGY DEVELOPMENT TOOL. SOURCE: ABOUT MMOWGLI, 2015.[204]

Another issue was that the government was unable to provide adequate coordination of all relief efforts. Jan Voordouw, Haiti-based coordinator for Cordaid, explains that in the wake of a crisis, coordination should normally be provided by the local government. However, in the case of Haiti, the government was "hard hit and could not do much."[205] A lack of accountability on the part of Ushahidi towards the government was the result. Nevertheless, Ushahidi Haiti did try to establish partnerships with the government. While the government was interested in closer cooperation, it cited structural problems that would stand in the way of new cooperation – chief among them being the lack of "a building or offices to set this up."[206] Despite this failure, Ushahidi still intended to hand over administration of the project to Haitians as soon as possible. An Ushahidi Field Representative was sent to Haiti for this specific purpose.[207] In November 2010, the coordination of Ushahidi Haiti was fully transferred to a Haitian software company called Solutions. The reconstruction mapping tool later started functioning under the label "Noula".[208]

4.2 BENEFITS OF USING USHAHIDI

Despite the absence of extensive quality assurance measures during the Ushahidi Haiti deployment and the resultant risk of errors, some sources claim that Ushahidi Haiti had a tremendous impact on the outcome of the relief operation.[209] Fast mobilization is one of the most frequently cited advantages of initiatives that involve local communities and international volunteers in HROs.[210] Ushahidi Haiti was set up a mere two hours after the earthquake struck and helped the relief community move into action swiftly.[211] It could become fully operational quickly given that the most important source of labor – the volunteers – was readily available. Traditional relief organizations that rely on verified official sources of information risk "running miles behind" since "the info is already available to the public [through crowdsourcing initiatives]."[212]

Additionally, in the first phases of the project, Ushahidi Haiti hardly required any financial support for its initiative. The web platform was taken care of by the software company Ushahidi, and the volunteers initially operated out of the apartment of one of the participants in Boston and only later moved into a place that was donated to the team.[213] Volunteers worked for free and, given that many of them were strongly motivated to contribute to the effort, there was no need for an extensive and costly media campaign to recruit people. As other actors realized the potential of the campaign, financial donations began to pour into the Ushahidi Haiti project. In total, around $97,000 was provided to Ushahidi. The majority share of this sum was invested into the actual operation in order to improve output and help ongoing efforts.[214]

Low operating costs are one of Ushahidi's strongest assets. Some financial resources are needed to employ staff, yet these are provided by the company itself and by means of donations. The relief organization, or any other cooperating partner who wishes to maintain this cooperation in the future, does not have to spend too much time or financial resources on the platform itself. Volunteers stop cooperating as soon as a particular operation is completed and new volunteers are recruited when a situation worsens in a particular area of the world. Ushahidi is therefore self-perpetuating; the basic motivation of volunteers to help the affected community will drive human willingness to help crowdsource the data. In the end, the volunteer, located far away from the disaster area, has oftentimes no alternative other than helping through a computer and the internet.

Another advantage of cooperating through a platform such as Ushahidi are the low entry barriers. First, any individual can choose to join the volunteer community and contribute to making a crisis map. Volunteers were recruited from all over the world

and the type of cooperation that is established between the "mapper" and the platform is truly open in nature; anyone can join irrespective of his or her level of knowledge. And second, due to the fact that the final product is a freely available map, any relief organization or worker can easily use it or start a new collaboration initiative. Ushahidi's impact is ultimately evaluated according to the number and importance of relief actors that decided to use the platform.

The reason why this initiative managed to recruit so many volunteers was the feeling of helplessness that many individuals experienced. Especially for those who had an attachment to the Haitian community, it was painful to watch the island suffer from the comfort of one's own house. This desperate feeling was overcome by creating a real-time map of events.[215] Volunteers could quickly see the effects of their work, and even though they were not materially incentivized a word of gratitude served as a more than sufficient reward. Also the fact that internet and basic hardware are abundantly available in many places of the world made the volunteers eager to contribute. It also required little effort to join the initiative as the only sacrifice from their side was time.

The map of Haiti that the volunteer community developed in the course of a couple of weeks is of remarkable quality. The effort was successful to such a point that Craig Fugate, a member of the FEMA Task Force, tweeted that "[t]he crisis map of Haiti represents the most comprehensive and up-to-date map available to the humanitarian community."[216] The main difference between this map and the maps that were available to the relief community from other sources was that the crisis map contained data about actionable reports – a map that had not been developed prior to this disaster.[217] Figure 9 provides a comparison of how the OpenStreetMap of Haiti looked before the earthquake and after the volunteer initiatives were concluded.

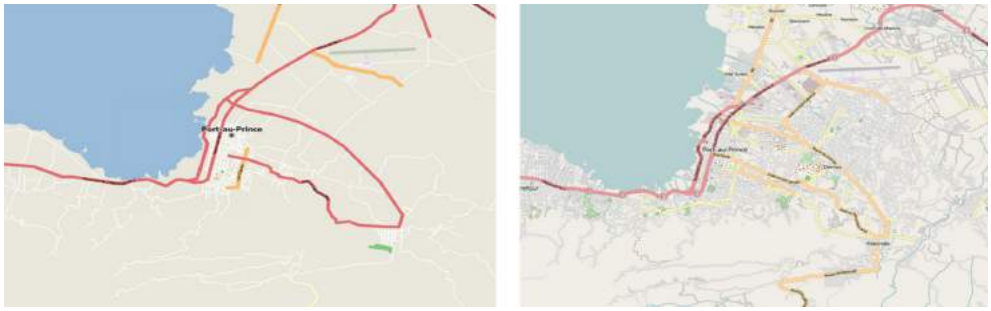

FIGURE 9: A MAP OF HAITI BEFORE AND AFTER THE 2010 EARTHQUAKE. SOURCE: OPEN KNOWLEDGE BLOG, 2010.[218]

The combination of a live crisis map and the generation of a new knowledge base that could be built quickly and at a low cost makes Ushahidi a very promising new platform. Among the organizations and entities that made significant use of the Ushahidi Haiti data were the US Marine Corps, numerous other US governmental bodies (US Department of State, the US Coast Guard, the Office of US Foreign Disaster Assistance and the Federal Emergency Management Agency), non-profit organizations such as NYC Medics, the UN World Food Program and American, and Canadian citizens engaged in relief operations.[219] The US Marine Corps used the geodata for the identification of centers of gravity where marines should consequently be sent to (see Figure 10 on how the US Department of Defense uses big data in ensuring a more effective on-the-ground operation).[220]

PREDICTING THE FUTURE WITH CROWDSOURCING

The fact that involving large numbers can make a difference in producing more precise input for policy-making or on-the-ground operations, in particular in combination with other data sources, is seen in the US Department of Defense's *Intelligence Advanced Research Projects Activity (IARPA).* It has been established for the purpose of collecting big data and proved relevant in responding to epidemics, the Arab Spring, or the Islamic State.[i] But IARPA also announced a competition whose winning project, *Aggregative Contingent Estimation System* (ACES), asks the public about intelligence strategies and produces more accurate forecasts.[ii] Should the number of predictors increase in the future, ACES would be apt at developing strategies of advanced analytics of big data that has been directly crowdsourced from the broad public.

FIGURE 10: PREDICTING THE FUTURE WITH CROWDSOURCING. SOURCE: CORRIN, 2015; PARSONS, 2011.

The importance of Ushahidi Haiti for the relief operation is perhaps best illustrated through personal testimonies of relief workers directly involved. Clark Craig, a former JAG attorney in the US Marine Corps, has expressed his gratitude for the project in these words:

"I cannot overemphasize what the work of the Ushahidi-Haiti has provided. It is saving lives every day. [...] I say with confidence that there are hundreds of these kinds of [success] stories. The Marine Corps is using your project every second of the day to get aid and assistance to the people that need it most. [...] Keep up the good work! You are making the biggest difference of anything I have seen out there in the open source world."

Hillary Clinton stated that with the help of "interactive maps, [...], a seven-year-old girl and two women were pulled from the rubble of a collapsed supermarket by an American search-and-rescue team after they sent a text message calling for help."[221]

4.3 DRAWBACKS OF USING USHAHIDI

Despite all the benefits of using Ushahidi Haiti, a conclusive judgement on the success of the project proves hard to make. There were a number of issues that stood in the way of a more effective cooperation between the relief community on the one hand and Ushahidi Haiti on the other. These concerns included issues of coordination, data, technology, accuracy and credibility, exposure, and privacy.[222]

Coordination can be a challenge when it comes to open and informal types of cooperation. Volunteers operate in a largely uncoordinated manner and crowdsourcing initiatives lack an overarching authority to steer individual actions. When a report is posted on the Ushahidi website, any relief organization has access to it. However, to decide which organization should take action is more difficult. There are no formal mechanisms for dividing the work among organizations, causing situations wherein more than one actor responds to a concrete report.[223] This also means that it is difficult to evaluate the impact of a project as there is no proper way of providing feedback or testifying whether help was provided or not. Finally, because the eventual map blends together all the info provided by all the different organizations, the contribution of each to the map is hard to establish – and thus so is the value of their real contribution.[224]

Rather than coping with a lack of information during a humanitarian crisis, crowdsourced initiatives such as Ushahidi tended to be faced with an information overload.[225] Some stakeholders felt that the data analysis skills of volunteers might be insufficient to process and categorize all reports that were available and therefore only contribute to a more chaotic database. Specifically, stakeholders felt Ushahidi Haiti provided insufficient coverage on security and logistics. For instance, many reports contained a lack of detail to allow them to be considered actionable and were eventually not used. Out of the estimated 40,000 to 60,000 reports, only 3,584 were put on the crisis map[226]; only fifty-four of these were categorized as pertaining to security threats.

In terms of accuracy and credibility, concerns about the accuracy of crowdsourced information existed well before Ushahidi's inception. Ory Okolloh, Ushahidi's co-founder, was aware of the fact that there would be instances where reports would be found to be incorrect or contain duplications, but she argued that having access to at least some – admittedly not 100% correct – information is better than having no access at all. David Kobia, another one of Ushahidi's co-founders, expressed his belief that whereas sometimes a greater accuracy of data is required, there are many other circumstances where an accumulation of more data is in fact preferred over absolute

precision. He gives an example of the UN, which also realized that achieving perfect data accuracy is an unattainable goal. Data precision according to Kobia is that "the crowd validates itself and says what did or did not happen."[227]

Back in 2007, the first Ushahidi reports had to be checked manually and could only be marked as verified when the source was proven to be reliable.[228] The Haitian earthquake, however, represented a disaster where people were in need of immediate help and where people's lives were directly threatened. This may have been one of the reasons why the Ushahidi Haiti team decided not to employ extensive quality controls at this stage. However, inadvertently this led to higher instances of data inaccuracy, in particular the occurrence of duplicate reports and those whose categorization contained errors.[229] However, according to the US Coast Guard, the part of the dataset that was processed correctly provided geographic coordinates that were accurate up to 5 decimal points.[230] That said, the impossibility of verifying the quality of the information during the Haiti deployment was a primary concern among many organizations and stakeholders in considering the use of crowdsourced data.[231]

Ushahidi relies on volunteers who are oftentimes inexperienced and therefore prone to making mistakes. Volunteers sometimes struggled with the categorization of reports that did not fit in a specific category but were nonetheless urgent. In those cases, volunteers would intentionally wrongly categorize these reports only to make sure that they would be recognized and deemed actionable. This kind of data manipulation has been cited as a concern by some members of the relief community. Ushahidi Haiti also struggled with double reporting. More than a hundred reports were identified as duplicates.[232]

Also, the medium itself may have an influence on the way information is received and treated. A study by Schultz, Utz, and Goritz shows that social media is viewed as a credible source (especially in the context of a humanitarian crisis) due to its agile and responsive nature.[233] However, despite the amount of information available, there is often insufficient detail provided by those who report on the issue at hand. Many messages and reports received by Ushahidi were incomplete or indecipherable.[234] There is the additional risk that reports can be fake or that people from the community have manipulated the information that is inserted into the map.[235]

As a result, the relief community is reluctant to use user-accumulated data. Generally speaking, the relief community relies on "standard procedures using structured indicator data" and "long-standing protocols." Unless the data has been organized

through the United Nations system, relief workers simply do not have time to consider unverified sources of information in their response to disasters.[236] This translates into strict expectations about the data received in terms of the format and time needed for processing. These expectations are perhaps impossible to meet by the volunteer community. This discrepancy between open source output and the relief community's norms and standards often means that organizations simply choose to "stay in [their] comfort zone," as stated by an American official.[237]

These shortcomings notwithstanding, crowdsourcing initiatives are increasingly recognized as possessing value and organizations such as the US Joint Chiefs of Staff, the Clinton Foundation, UNDP, and the UN Interagency Standing Committee are looking into ways to incorporate "crowd wisdom" into their operations.[238]

Online platforms such as Ushahidi inevitably raise privacy and security concerns. Volunteers, in processing the data, also gain access to sensitive information. Moreover, reports are freely accessible on the internet, and this became a point of disagreement between Ushahidi Haiti and other volunteer initiatives, such as Mission 4636. While the latter decided to protect the senders, Ushahidi Haiti was initially publishing reports online that included the names of the authors.[239] It soon became clear that this practice exposed vulnerable groups and individuals, thus compromising their privacy and safety.[240]

What is more, Ushahidi Haiti was one of the 50 websites monitored by the US Department of Homeland Security in order to gain material about potentially threatening persons.[241] What this essentially means is that Ushahidi Haiti was, instead of connecting the affected community with the relief workers on the ground, also inadvertently providing information to an American intelligence body. Some people who sent a message to the shortcode were at times not provided the aid they requested, yet were still scanned by the Department for intelligence information.[242] This issue can also endanger relief workers.[243] But it also raised questions among Haitians about involvement with crowdsourcing initiatives and whether this could compromise their own safety and security. Aashika Damodar, the co-founder of an alternative text messaging service Ayiti SMS SOS, said that when people do not feel safe, they will have concerns when considering whether to report or not.[244]

Crowdsourcing was also used by the UNDP in Latin America, Kenya, Sudan, and Kyrgyzstan. The way the public was engaged ranged from reporting security threats to providing opinions and perceptions of the current security situation.[245] While the UNDP

deployments were similar to Ushahidi in the limitations that they faced, there are some differences, notably with respect to privacy concerns. In Kenya, only the crowdsourced information was made freely available to the responders, while public access to information was restricted. Even though this would partly mitigate the privacy issues outlined above, it was identified as a limitation in the UNDP report.[246] Similarly to Ushahidi, in Latin America, citizens' concerns about privacy were one of the reasons for the unwillingness to report; crowdsourcing initiatives would likely have been more successful had there been a greater trust in the legal authorities.[247] The UNDP report states that "[p]rivacy should remain the number one concern when developing Big Data for development and [...] conflict prevention"[248] and that the development of "privacy-preserving data analysis" would benefit future crowdsourcing missions.[249]

4.4 IMPROVEMENTS

Ushahidi is a work in progress and each new deployment produces numerous lessons (to be) learned. It can be said that with Ushahidi, "innovation has happened basically in the midst of disasters, with time constraints, minimal resources and in the shadow of the more traditional roles of relief agencies and geographic professionals."[250] During the project in Haiti, many things changed over the course of the initiative. Many improvements were made, such as in the publication of sensitive reports. When it had become clear that vulnerable groups and persons were exposed, Ushahidi Haiti recognized the mistake and stopped publishing full reports online. The nature of Ushahidi is to be fully transparent, open, and participatory, and this was the driver behind the decision to publish messages online. However, compromising the protection of senders was identified as a gravely negative byproduct of the open policies and eliminated from the project. While Ushahidi was open to criticism and changed the previous behavior, unveiling too much private and sensitive information remains an issue of concern.[251]

The lack of accuracy has been quoted many times as a problem. The overall low percentage of verified reports is a discouraging element for new actors to cooperate with Ushahidi in the future. However, there are instruments that can ameliorate the overall trustworthiness. Especially when monitoring post-electoral situations, Ushahidi is employing a tactic of building a network of "trusted reporters" – people whose contribution is considered reliable. Hence when building a map, reports from this network do not need to be checked before entering the database, while other, unverified reports are pending approval.[252] Furthermore, the plugin "SwiftRiver" was developed to filter the large amounts of data and ensure their accuracy. However, the Ushahidi team decided to stop developing this plugin as of January 5, 2015.[253]

The new version of Ushahidi, V3, also features more comprehensive quality assurance measures. Ushahidi introduces "modular quality assurance", which focuses on individual parts of the website – the patterns – rather than on the website as a whole. Ensuring that the pattern is correct would also contribute to the quality of Ushahidi websites.[254] However, the developers are aware of the potential errors in any open source tool and are constantly asking for feedback and support with ensuring the accuracy of Ushahidi's reporting.[255] The website even has a group called "SWAT" that was specifically created to recruit skilled developers and other volunteers who believe they have the eye to spot and fix the bugs in Ushahidi's reporting system.[256]

As stated above, the category "security" was underrepresented in the Ushahidi Haiti project. Ushahidi realized that the category itself must have been underreported to a certain degree. An explanation could be that people who are in an immediate life threat do not have the time or tools to send a report.[257] Ushahidi's field representatives were sent to Haiti to find solutions in cooperation with the local and international relief workers. The impersonality and scarcity of rich reports have been resolved through the establishment of call centers as a part of another crisis mapping initiative in Haiti, Noula. This is, however, not applicable only to Haiti. The talks between Ushahidi and the relief community have been useful in bringing the two sides together and brought a framework of how the cooperation could move forward in the future crises. This could have contributed to an institutionalization of the way Ushahidi can be used in crisis management.[258]

A new feature of Ushahidi, which was not present during the Haiti deployment, is a function that enables relief workers to get alerts through their preferred channel (either SMS or email). These alerts can be based on the category of the reports or on geography. This function will contribute to matching the reports with the responders in a more efficient and effective way and will enhance the overall impact of Ushahidi in future deployments.[259]

Categorization of reports is one of the most important features of Ushahidi's maps and even though categorization did occur during the Haitian earthquake, this process was rather arbitrary. It would undoubtedly contribute to the overall quality of Ushahidi's maps if flagging and labeling the reports according to their urgency and nature would be determined by a more sophisticated way than the mere judgement of a volunteer. Triaging these reports with an algorithm or in another automated way could eradicate errors and speed up the process.[260]

Perhaps most importantly, the Ushahidi blog reveals that, "The unprecedented response of online volunteers during the 2010 Earthquake in Haiti introduced new processes, tools, and actors to the humanitarian landscape but also brought new challenges: chiefly among them being coordination of information and efforts."[261] In other words, Ushahidi realized that the best way to help might be not to contribute to the number of already existing volunteer efforts but to support those who are trying to organize and coordinate these projects. This is the reason why Ushahidi did not actively involve its platform in the Nepal 2015 earthquake. Instead, Ushahidi initiated partnerships with colleagues from the crisis mapping community and decided to support their efforts, calling on their own volunteers to do the same. What has been done since the Haitian earthquake in this matter is the establishment of the Digital Humanitarian Network to serve as a bridge between the two sides: traditional relief organizations and new volunteer platforms. This network has already published two documents that aim to ameliorate the coordination of efforts: *Guidance for Collaborating with Volunteer & Technical Communities* and *Guidance for Collaborating with Formal Humanitarian Organizations*.[262]

4.5 APPLICABILITY FOR NDOs

The importance of situational awareness for NDOs is a given that requires no elaboration. To create and maintain situational awareness, NDOs invest heavily in advanced sensor and information systems (including humans-in-the-loop). There are, however, many situations in which these systems are not or may not be deployed. Furthermore, advanced as these systems may be, in many scenarios they are insufficient for gathering all relevant information. That is where the idea kicks in of using people already on the ground to provide and augment the information available through one's own channels: people that know the local situation and generate real-time information. People that not only see but also can give context to what they see, thereby contributing to situational understanding on top of situational awareness. With ubiquitous communication means – mobile devices with GSM or internet connectivity – available, reaching out to reporters on the ground is increasingly feasible. Modern geospatial and data processing tooling facilitate better combination, visualization, and correlation of the data so obtained, allowing for easy quality enhancing feedback loops.

An open, on-line crisis situation map that is generated or augmented by continuous input from volunteers on the ground offers the following advantages for a military crisis response task force:

- By using the local community as a source of information the map is *more comprehensive and up-to-date* than anything the military can generate on their own;
- *Fast mobilization*: volunteers are ready to help as soon as possible (when sufficiently motivated);
- There are *little to no entry barriers*. Anybody can choose to join the volunteer community and any relief organization or worker can easily use it or start a form of collaboration;
- Volunteers need no extrinsic incentives and *little or no financial support*. There are also *low maintenance costs*: volunteers stop cooperating as soon as a particular operation is completed, and new volunteers are only recruited when needed.

Ushahidi Haiti is a case in point. Its aim was to create a crisis map that could help relief workers in their rescue operations. While the impact of the map is difficult to determine, a comprehensive map of the island was certainly created. Platforms such as Ushahidi carry a high potential when it comes to monitoring security situations. Above all, an online platform adds a source of relevant information above and beyond what NDOs already have access to. They address time and resource constraints as a basis for action-oriented decision making. Furthermore, it is a source that can be mobilized quickly and generates (near) real-time reporting. In some cases, it offers a way to circumvent government censorship and propaganda. And all of this against very limited costs.

The Ushahidi example shows that life-saving information-gathering operations based on crowdsourcing can be set up and operational within hours after disaster has struck. Related to this is that the resources needed to set up these operations may not be available immediately, or even at all. The fact that Ushahidi relies on volunteers drastically reduces the costs involved. Finally, Ushahidi has already demonstrated that it can be a useful monitoring tool for security purposes over the course of the 2007/2008 post-electoral violence episode in Kenya. In such circumstances, local knowledge can be helpful, especially when censorship and propaganda are imposed on independent sources of information.[263]

The potential and actual disadvantages to the use of platforms such as Ushahidi to create online crisis situation maps are:

- *Coordination is difficult*, in particular when many parties – such as individual citizens, government agencies, local NGO's, and the relief community – are required to generate a comprehensive map;
- Both *information overload and/or insufficient coverage* may arise from too much or too little reporting;
- Human errors, a lack of actionable reports, double reporting, or a lack of verification possibilities etc. may lead to a map / database of *questionable quality*. Gross inaccuracies inadvertently give rise to trust issues and people feeling disinclined to use the platform – a vicious circle that is difficult to stop;
- *Insufficient technological equipment* – such as web browsers, internet connection of the relief community – may lead to underdeveloped or underused maps;
- *Resistance and lack of exposure*: the entry barriers for joining the platform might be high for the traditional relief community. If insufficiently known or accepted, resources must be invested in promoting the platform;
- Information is processed by volunteers and reports can be freely accessed through the internet. This raises *issues of security and privacy*.

Many of these limited factors can be successfully addressed or mitigated. Our example case, Ushahidi, is a work in progress platform and each new deployment produces new lessons learned. The Ushahidi blog states that "[t]he unprecedented response of online volunteers during the 2010 Earthquake in Haiti introduced new processes, tools, and actors to the humanitarian landscape but also brought new challenges: chief among them being the coordination of information and [ongoing] efforts."[264] In other words, Ushahidi realized that the best way to help might be not to contribute to the number of already existing volunteer efforts, but to support those who are trying to organize and coordinate these projects. This is the reason why Ushahidi did not actively involve its platform in the Nepal 2015 earthquake. Instead, Ushahidi initiated partnerships with colleagues from the crisis mapping community and decided to support their efforts, calling on their own volunteers to do the same. What has been done since the Haitian earthquake in this fashion is the establishment of the Digital Humanitarian Network to bridge the gaps between traditional relief organizations on the one hand, and new volunteer platforms on the other. This network has already published two documents that aim to ameliorate the coordination of efforts: *Guidance for Collaborating with Volunteer & Technical Communities* and *Guidance for Collaborating with Formal Humanitarian Organizations*.[265]

4.6 PRACTICAL EXAMPLES

Ushahidi Haiti inspired a variety of organizations to make use of the digital environment in crisis management and disaster response. The US Department of State was actively involved in the Haitian relief operation and cooperated with the Ushahidi Haiti project. In doing so the Department recognized that the use of online technologies had a positive impact on the outcome of the relief operations and decided to implement these in their future humanitarian efforts. "TechCamps" were established around the world to connect NGOs and experts in the field of technology in order to find creative solutions to humanitarian problems. According to the director of the US State Department's eDiplomacy, the TechCamps are "a way to identify the next Ushahidi or FrontlineSMS and help them scale quickly."[266] This represents a shift from a more closed view on resolving humanitarian issues to involving the community at large. USAID has also welcomed the initiative and its Chief Innovation Officer expressed his belief that through "mashing up local insights and tech tools," the new project will "save lives, create stable and open governments, and greater prosperity for all".[267]

The Ushahidi platform has been successfully used in various countries and operations after the earthquake.[268] Ushahidi has learned from its past deployments and aspires to respond to the changing environment and constantly improve itself. The platform undoubtedly has many shortcomings, and a NDO wishing to cooperate with and use Ushahidi must be aware of all its (potential) benefits and risks. However, it cannot be denied that Ushahidi provides an excellent opportunity for true innovative partnerships. Ushahidi and similar platforms thus deserve a place in the field of defense and security.

The applicability for NDOs is obvious when it comes to missions that have clear popular support in the area of operations, as in the case of (military support to) humanitarian relief operations. One can also envisage the use of this mechanism in scenarios other than a clear and present emergency situation. An example could be to augment situational awareness about potential hotspots where a security risk might develop into an actual security threat or conflict. Possibly the lack of an intrinsic sense of urgency requires the establishment of an incentive structure to motivate possible contributors.

5 SO WHAT FOR DEFENSE?

5.1 COOPERABILITY IS BECOMING THE KEY SOURCE OF COMPETITIVE ADVANTAGE 100
5.2 MONITOR AND EXPERIMENT WITH NEW FORMS OF COOPERATION TECHNOLOGIES 101
5.3 SEE COOPERATION AS A PORTFOLIO CHOICE 102
5.4 LESSONS FROM THE CASES 102

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.

6 FINAL OBSERVATIONS

6 FINAL OBSERVATIONS

In an ever more connected and complex world, fostering a more diversified portfolio of cooperation partners and cooperation forms has become a strategic imperative for NDOs. The scope of these modern cooperation networks transcends far beyond the traditional alliances with likewise organizations.

Richard Nelson, an eminent professor of economics at Columbia University in New York, differentiates between what he calls "physical" – e.g. steel, energy, etc. – and "social" technologies – e.g. institutions, forms of cooperation, etc. Most major societal advances result from the evolutionary interplay between physical and social technologies.[271] One of Nelson's important insights is that our societies' "ability to develop effective social technologies is more limited and more prone to frustration that [their] ability to advance physical technologies."[272] It took many decades before the physical technological breakthroughs that irrupted into our societies and gave rise to the industrial revolution engendered new social technologies such as factories, private firms, the concept of 'division of labor' etc. Early steam engines were already pumping water out of coal mines and coking coals were already being used to melt iron in the early 18th century – but the consolidation of these efforts into 'factories' only started happening in the second half of that century.[273] The emergence of the modern firm – often in close cooperation with that other major emerging social technology, the modern state – also occurred in this very same period. Great Britain was the first country to stumble upon the right balance between physical and social technologies in this case. It was able to parlay this ingenuity into global dominance for over a century. A similar trend could also be observed in the military realm, where those nations that were able to decipher the new social technological codes that were embedded in industrial-age physical technological breakthroughs gained an enormous operational and strategic advantage over those that were not.

As was the case with the transition from the agricultural to the industrial age, physical technologies seem to once again run ahead of social technologies. The, so far still mostly physical, ICT revolution brings dramatic change to many areas of public and private life. Snowballing nano-, bio-, info-, and cogno- revolutions[274] may very well soon start accelerating the pace and scope of this change even more. Changes in these physical technologies are occurring much more quickly than in any previous age, and there are good reasons to believe that they are likely to accelerate even more – especially if they start building on each other.[275] It is important to point out that the information-heavy nature of these ongoing revolutions differs quite markedly from the information-light nature of the physical technologies that engendered the industrial revolution.[276]

The industrial age ended up being very different from any of the previous ages. The machines, capital investments, training requirements, even the mindset of the industrial age all required mass. Every sphere of public and private activity witnessed a sizeable expansion in scope. The mostly small pre- and proto-industrial economic agents mushroomed into factories. Many smaller pre-Westphalian geopolitical entities matured into nation-states. Also in the defense world, the scope of military units, organizations, operations, etc. witnessed major increases in size. The massive NDOs as we witness them today came into being.

It remains as of yet unclear to what extent mass will prevail in the post-industrial age. We currently still see massive post-industrial behemoths such as Google, Apple, or Microsoft taking advantage of their economies of scale and scope to creep into the top-50 of the largest companies.[277] Are they the heirs of an industrial revolution based on mass that will be able to leverage their first-mover advantages into new, dominant (but probably still differently so) global behemoths? Or will the future be dominated by the new types of more distributed, peer-to-peer organizational forms based on different business models that we have described in this report – such as open source software in areas such as web servers (Apache), operating systems (Linux), etc.; such as peer-to-peer sharing initiatives such as Airbnb, Uber, Kiva etc.; or maybe even new manufacturing initiatives such as 3D fablabs and Etsy?

Irrespective of which type of organizational principle will end up generating most value, it seems virtually inconceivable that all of these new physical technological breakthroughs will not lead to dramatic new forms of social technologies – of which some of the examples we sketched here may be early precursors. It may be useful to emphasize that the participants in some of these new forms of cooperation are not

just some bit-players in marginal sectors. The pharmaceutical sector, such as the defense sector, is a massive capital-intensive industry with an extremely globalized and sophisticated value chain in which R&D plays a critical role. The fact that it has opened itself (selectively) to new forms of cooperation is quite telling. NDOs would therefore be well advised to open up their organization and be prepared – and more so, actively search – for unexpected new ways and partners for working better together.

ANNEX A: A FIRST DRAFT TAXONOMY OF COOPERATION

ANNEX A: A FIRST DRAFT TAXONOMY OF COOPERATION

Cooperation is an important topic of inquiry in many different academic disciplines. Biological lifeforms cooperate. Economic agents cooperate. Political movements and parties cooperate. States cooperate. Defense organizations cooperate. It seems that that in all of these diverse forms of cooperation we find back the entities that cooperate (who?), the purpose of their cooperation (why?), the nature of their cooperation (what?), the interfaces between them (how/through what?), and the broader system within which they cooperate (where?). Of course, the labels that are given to these elements differ from discipline to discipline. 'The who', for instance, goes by different names in different fields:

- 'agents' in economics, computer science and game theory/public choice;
- 'actors' or 'organizations' in polisci;
- 'humans' or 'groups' in anthropology, psychology and sociology;
- 'parties' in legal sciences,
- 'nodes' in network and related sciences, 'components',
- 'elements' in many natural sciences

All of these different labels refer to the same category of (deliberate or undeliberate) 'agency' which represents the active units that engage in cooperation.

For each of these broad categories, we have identified a number of 'parameters' along which types of cooperation may vary. These in essence represent a number of different 'dimensions' of the 'cooperation space'. Some of these parameters have been elaborated in terms of description, a way of operationalizing it, our assessment of where NDOs typically stand along that operationalization, and our assessment of what we see happening in the world in the non-defense sector.

The listing below is nothing but a try-out, an incomplete first exercise. We do not intend or pretend to be exhaustive. But we also do not want to limit ourselves to a few high-level abstract parameters that may still hide some meaningful difference that may matter to DSOs. We want them to be 'discrete' enough to allow us to select a few where we really observe new forms of cooperation appear and thrive 'in the wild' – where applicable and interesting also within, still but predominantly outside of the defense realm.

(NATURE OF THE) INTERACTORS – THE WHO?

- **Size**: in most systems, some elements tend to be bigger, like-sized or smaller
  Operationalization: big<->big ; big->small ; small -> big ; small <-> small
  Defense now: since DSOs tend to be big, their current forms of interaction tend to skew towards the left side of this spectrum. Examples of big-big include: with other defense organizations; with other government departments; with big defense companies. Examples of big-small include: with smaller contractors on specific issues (catering, nice capabilities); with smaller force providers (e.g. Afghan warlord forces).
  Trend in the wild: much more diversity (main driver: lower transaction costs) – e.g. 'swarms' of small ones that interact with the big ones as (near)-peers

- **Number of decision makers**: all members of an organization may be involved in interaction decisions. Alternatively, only some members fulfil this role
- **Scope**: some organizations tend to have a very broad scope (e.g. in the business world big conglomerates (keiretsu, chaebols; in networks free-scale networks; etc.), others very narrow (niche companies,
  Operationalization: broad<-> broad ; broad ->narrow ; narrow -> broad ; narrow <->narrow
  Defense now: leaning towards the right: defense is fairly delineated in what it thinks it should or should not do, and there aren't many really 'broad' cooperation partners (the UN would be the one broad example that springs to mind)
  Trend 'in the wild': again more diversity (main driver: lower transaction costs) e.g. Google constantly scanning (globally!) smaller nice players and sometimes buying them out, sometimes just working with them
- **Homo-heterogeneity**: whether the interactors are homogeneous by nature or heterogeneous
- **Structure**: hierarchical or not?; stovepiped or not?
- **Nature**: cohesive or not? status-quo or not?

(PURPOSE OF THE) INTERACTION – THE WHY?

- **Aim**: Why do agents cooperate?
  Operationalization: For operational effectiveness, for efficiency gains, for 'what-if' scenarios [for evolutionary biology the aim is ultimately an increase in inclusive fitness]
- **Equity (cui bono?)**: are benefits (and/or costs) of cooperation fairly distributed or not
  Operationalization: ? (e.g. in ecology – mutualism, commensalism, amensalism and parasitism)

(NATURE OF THE) INTERACTION – THE WHAT?

- **Purposive or non-purposive**: do they purposefully want to cooperate with others or do they just end up cooperating de facto
- **Coalitional size**
  Operationalization: dyadic/2, mini-lateral, medi-lateral, maxi-lateral
- **Freedom of choice**
  Operationalization: voluntary or non-voluntary (coerced) or unintentional
- **Symmetrical or not**: Does one need the interaction a lot more than the other one?
- **Hierarchical or not:** is there a 'stronger'/more powerful one and a weaker/less powerful one
- **Partner choice**
  Operationalization: inside-out ('we' choose), outside-in (they choose us) or mutual.
- **Temporal**
  Operationalization: acc-incidental/ad-hoc, or structural/long-term
- **Adaptivity**
  Operationalization: Rigid (fixed) or adaptive (flexible)
- **Substantive:** what is the interaction all about?
  Operationalization: value-based (Weber – gemeinschaft vs gesellschaft; e.g Karl Deutsch' security community); purpose-based (do they share similar or identical objectives/purposes)?; incentives-based (do they share some – maybe transient) incentives; purely instrumental (just about sharing resources)
- **Trustworthiness and trust**: evaluation of actions in relation to prior stated intentions.
  Operationalization: evaluation of self by the other interactant(s) and potential interactants (= trustworthiness), and vice versa (= trust) based on history and current behaviour. Reputation. Distinguishing honest from deceptive signals.

(Nature of the) Interface – the how / through what?

- **Information exchange and decision making:** is decision making preceded by information exchange and/or discussion? Are decisions made alternately by each side (or sequentially by all sides if more than two), simultaneously or something more complex where there are more than two parties? How are decisions made within a group or organization? How are negotiations between groups managed?
- **Formal/informal**
- **High-cost/low cost:** costs to all parties and symmetry/asymmetry of these costs
- **Types of cost:** the nature of costs to the parties involved. We can distinguish between 'interaction costs' (intrinsic to the interaction and unavoidable to a variable degree) and 'outcome costs' (which depend on the outcome of the interaction)
  Operationalization: Interaction costs: Cognitive (for the individual) and 'informational requirement' (for the organization) costs of the interaction. Outcome costs: money, time, energy, sharing of previously private information, loss of reputation.
- **Loose or tight:** the term 'loose coupling' comes originally from the IT sector, from whence it expanded into many other disciplines[278].
- **Enforceable or not**

(Nature of the) Interaction Context/Environment – where?

- **One- or two-way**
  Operationalization: one-way (the environment influences the interaction or the outcome of the interaction influences the environment) or two-way. The (social) environment includes other potential interactants in the environment
- **Stable vs dynamic/turbulent**
- **Rules/norms/standards-based or not**

BIBLIOGRAPHY

BIBLIOGRAPHY

"$1 Million Prize Awarded for New Algorithm for Rapid Characterization of Pathogens." *InnoCentive*, March 12, 2013. http://www.innocentive.com/1-million-prize-awarded-new-algorithm-rapid-characterization-pathogens.

"About MMOWGLI." *MMOWGLI Portal*. Accessed October 7, 2015. https://portal.mmowgli.nps.edu/game-wiki/-/wiki/10773/About+MMOWGLI.

"About Open Innovation." *EIDON Lab*, October 10, 2011. http://www.eidon-lab.eu/index/index.php?option=com_content&view=article&id=66&lang=en.

Allen, Nick. "Hit Men, Drugs and the Fall of Ross Ulbricht, the Silk Road 'Mastermind.'" *The Telegraph*, October 4, 2013. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10356444/Hit-men-drugs-and-the-fall-of-Ross-Ulbricht-the-Silk-Road-mastermind.html.

"APT28: A Window Into Russia's Cyber Espionage Operations?" Milpitas, CA: FireEye, October 2014. https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf.

Baregheh, Anahita, Jennifer Rowley, and Sally Sambrook. "Towards a Multidisciplinary Definition of Innovation." *Management Decision* 47, no. 8 (September 4, 2009): 1323–39. doi:10.1108/00251740910984578.

Barton, Bob, and Dick Whittington. "Meeting Capability Goals through Effective Modelling and Experimentation of C4ISTAR Options." presented at the ICCRTS 16, June 2011. http://www.dodccrp.org/events/16th_iccrts_2011/presentations/007.pdf.

Basilaia, Mikheil. "Volunteers and Cyber Security - Options for Georgia." Tallinn University of Technology, 2012. http://csbd.gov.ge/doc/Volunteers%20and%20Cyber%20Security%20-%20Options%20for%20Georgia.%20Mikheil%20Basilaia.pdf.

Beinhocker, Eric. *The Origin of Wealth: Evolution, Complexity, and the Radical Remaking of Economics*. Boston Mass.: Harvard Business School Press, 2006.

Bishop, Michelle. "The Total Economic Impact Of InnoCentive Challenges: Single Company Case Study." Forrester Comsulting, January 5, 2009. https://www.innocentive.com/files/node/casestudy/total-economic-impacttm-innocentive-challenges-sca-case-study.pdf.

BlackEnergy & Quedagh: The Convergence of Crimeware and APT Attacks. F-Secure, 2014. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.

Blackford, Mansel G. *The Rise of Modern Business: Great Britain, the United States, Germany, Japan, and China*. UNC Press Books, 2012.

Bodeen, Christopher. "Chinese Hackers Take Weekends Off." *The Huffington Post*. February 25, 2013. http://www.huffingtonpost.com/2013/02/25/chinese-hackers_n_2756914.html.

Booker, Dawn S. "Wiki Approaches to Wicked Problems: Considering African Traditions in Innovative Collaborative Approaches." *Development in Practice* 24, no. 5–6 (August 18, 2014): 672–85. doi:10.1080/09614524.2014.934786.

Bourgon, Jocelyne. *A New Synthesis of Public Administration Serving in the 21st Century*. Montreal: McGill-Queen's University Press, 2011. http://site.ebrary.com/id/10577863.

Boyd, E. B. "State Department Is Trying To Make A Thousand Ushahidis Bloom." *Fast Company*. Accessed September 15, 2015. http://www.fastcompany.com/1751308/state-department-trying-make-thousand-ushahidis-bloom.

"British Defence-Acquisition Reform - The RUSI Journal - Volume 159, Issue 1." Accessed January 24, 2016. http://www.tandfonline.com/doi/abs/10.1080/03071847.2014.895256#.VqVFKIltAhM.

Brown, Jessie-May, and Pincher Martin. "Talon Strike – Securing a Clear View of the Battlefield." *Royal United Services Institute*, 2011.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, Inc., 2010.

"Challenge Specific Agreement." *InnoCentive*. Accessed October 2, 2015. https://www.innocentive.com/ar/contract/printUnsigned/36.

Charlie, Osborne, and Zero Day. "Google Recruits Top PS3 Hacker for Project Zero." *ZDNet*, July 2014. http://www.zdnet.com/article/google-recruits-top-ps3-hacker-for-project-zero/.

Chesbrough, Henry W. "The Era of Open Innovation." *MIT Sloan Management Review*, Spring 2003.

"China Says U.S. Hacking Accusations Lack Technical Proof." *Reuters*, February 20, 2013. http://www.reuters.com/article/2013/02/20/us-china-hacking-idUSBRE91I06120130220.

"China Takes Lead On The 2015 Global 2000." *Forbes*. Accessed October 26, 2015. http://www.forbes.com/global2000/list/.

Clayton, Mark. "Stealing US Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China." *Christian Science Monitor*, September 14, 2012. http://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China.

Coleman, E. Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London ; New York: Verso, 2014.

Conger, Cristen. "Could a Single Hacker Crash a Country's Network? - Estonia's Hack Attack." *HowStuffWorks*. Accessed September 9, 2015. http://computer.howstuffworks.com/hacker-crash-country-network.htm.

"Crimea – The Russian Cyber Strategy to Hit Ukraine." *InfoSec Institute*, March 11, 2014. http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.

"CTTSO Challenge: Pre-Event Insider Attack Recognition." *InnoCentive*, 2014. https://www.innocentive.com/ar/challenge/9933546.

Curtis, Devon. *Politics and Humanitarian Aid: Debates, Dilemmas and Dissension*. London: Humanitarian Policy Group / Overseas Development Institute, 2001.

Danchev, Dancho. "Georgia President's Web Site under DDoS Attack from Russian Hackers." *ZDNet*, July 22, 2008. http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/.

Davies, Andrew, Peter Jennings, and Mark Thomson. "One Defence: One Direction? The First Principles Review of Defence." Special Report. Barton ACT, Australia: Australian Strategic Policy Institute, 2015.

Davis, Jeffrey R., Elizabeth E. Richard, and Kathryn E. Keeton. "Open Innovation at NASA: A New Business Model for Advancing Human Health and Performance Innovations." *Research-Technology Management* 58, no. 3 (May 1, 2015): 52–58. doi:10.5437/08956308X5803325.

"Defence Industrial Strategy." UK Ministry of Defence, December 2005.

"Defensie en Thales onderhouden samen luchtruimverdedigings-systemen." *Defensie*, April 22, 2015. https://www.defensie.nl/actueel/nieuws/2015/04/22/defensie-en-thales-onderhouden-samen-luchtruimverdediging.

"Defensie Zoekt 150 'Cyber-Reservisten.'" *NU*, November 2, 2013. http://www.nu.nl/internet/3618029/defensie-zoekt-150-cyber-reservisten.html.

Department of Defence, Australia. *First Principles Review: Creating One Defence*. Canberra, Australian Capital Territory: Department of Defence, 2015. http://apo.org.au/research/first-principles-review-creating-one-defence.

Department Of State. The Office of Website Management, Bureau of Public Affairs. "Morocco." Report. Department Of State. The Office of Website Management, Bureau of Public Affairs., June 8, 2012. Moroccol. http://www.state.gov/e/eb/rls/othr/ics/2012/191203.htm.

De Spiegeleire, Stephan. "Ten Trends in Capability Planning for Defence and Security." *The RUSI Journal* 156, no. 5 (October 1, 2011): 20–28. doi:10.1080/03071847.2011.626270.

———. "Towards a Taxonomy of Cooperation," 2015. https://docs.google.com/document/d/1XUt3dPpX2UAuPlJsa1MtfdIXEykW15cpwYqC_Xzf9zM/edit?usp=drive_web&usp=embed_facebook.

de Spiegeleire, Stephan, and Eline Chivot. "Assessing Assertions of Assertiveness: The Chinese and Russian Cases - Reports." *HCSS Centre for Strategic Studies*, June 3, 2014. http://www.hcss.nl/reports/assessing-assertions-of-assertiveness-the-chinese-and-russian-cases/145/.

De Spiegeleire, Stephan, IBM INstitute for Business Value, Alan Baldwin, Frans Picavet, and John Reiners. "Commentary." In *Bridging the Collaboration Gap: Results from a Global Defense Survey on Collaboration During Coalition Operations*. Somers, NY: IBM, 2009. https://www.ibm.com/smarterplanet/global/files/us__en_us__government__gbe03231usen.pdf.

de Spiegeleire, Stephan, and Tim Sweijs. "Missile Defense - An Interactive Policy Analysis." *HCSS Centre for Strategic Studies*, July 11, 2011. http://www.hcss.nl/news/missile-threats-against-the-netherlands/309/.

"Diaspora Engagement in Humanitarian Response Paper." International Organization for Migration, May 2015. http://unobserver.iom.int/sites/default/files/FINAL%20Paper%20-%20Diaspora%20and%20Humanitarian%20Response%20-%20May%202015.pdf.

"Equipping the Army for the Future." *MooD Smarter Decisions*. Accessed January 28, 2016. http://www.moodinternational.com/casestudies_niteworks.html.

Finkle, Jim. "Russian Hackers Target NATO, Ukraine and Others: iSight." *Reuters*, October 14, 2014. http://www.reuters.com/article/2014/10/14/us-russia-hackers-idUSKCN0I308F20141014.

"Fortune 500 - Fortune." Accessed October 26, 2015. http://fortune.com/fortune500/.

Franklin, Thomas. "Home Phe Monitor Research Challenge Advancing the Treatment for PKU." 2013. http://npkua.org/Portals/0/PDFs/2014Conference/Home%20Phe%20Monitor%20Dr%20Tom%20Franklin.pdf.

"Frequently Asked Questions." *InnoCentive*, 2015. http://www.innocentive.com/faq/Solver.

"Frequently Asked Questions." *InnoCentive*, 2015. http://www.innocentive.com/faq/Solver.

Gaglioti, Frank. "Cuts to NASA Budget Gut Space Research - World Socialist Web Site." *World Socialist Web Site*, May 20, 2006. https://www.wsws.org/en/articles/2006/05/nasa-m20.html.

Gansler, Jacques S., and William Lucyshyn. "Reforming Acquisition: This Time Must Be Different." In *Proceedings of the Twelfth Annual Acquisition Research Symposium*. College Park, MD: Maryland Univ College Park Center for Public Policy and Private Enterprise, 2015.

Gao, Huiji, Geoffrey Barbier, and Rebecca Goolsby. "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief." *IEEE Intelligent Systems* 26, no. 3 (2011): 10–14.

Gerard, Jason R. "Defense Acquisition Reform: A Half-Century and Still Counting." Army Command and General Staff College, 2014.

Gharajedaghi, Jamshid. *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*. Amsterdam; Boston: Morgan Kaufmann/Elsevier, 2011.

Gigler, Björn-Sören, and Savita Bailur. *Closing the Feedback Loop: Can Technology Bridge the Accountability Gap?* World Bank Publications, 2014. http://public.eblib.com/choice/publicfullrecord.aspx?p=1711528.

Gilbert, David. "Ashley Madison Hack: Who Are Impact Team, Why Did They Leak Website Data and Will They Be Caught?" *International Business Times*, August 2015. http://www.ibtimes.co.uk/ashley-madison-hack-who-are-impact-team-why-did-they-leak-website-data-will-they-be-caught-1516328.

Giridharadas, Anand. "Ushahidi - Africa's Gift to Silicon Valley: How to Track a Crisis." *The New York Times*, March 13, 2010, sec. Week in Review. http://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html.

"GitHub · Build Software Better, Together." Accessed August 27, 2015. https://github.com/.

Gleick, James. *The Information: A History, a Theory, a Flood*. HarperCollins UK, 2011.

Goldstein, Joshua, and Juliana Rotich. "Digitally Networked Technology in Kenya's 2007–2008 Post-Election Crisis." Berkman Center Research Publication. Internet & Democracy Case Study Series, 2008. http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan042523.pdf.

Gray, Bernard. "Review of Acquisition for the Secretary of State for Defence: An Independent Report by Bernard Gray." Ministry of Defence of the UK, 2009.

Greenberg, Andy. "iPhone Super-Hacker Comex, Let Go From Apple, Goes To Work For Google." Forbes.com. *Forbes*, April 2013. http://www.forbes.com/sites/andygreenberg/2013/04/24/iphone-super-hacker-comex-let-go-from-apple-goes-to-work-for-google/.

Grevil, Frank S. "Gauging Sympathy for Snowden." *Consortiumnews*, July 3, 2013. https://consortiumnews.com/2013/07/03/gauging-sympathy-for-snowden/.

"Hackers Join In the Struggle for Crimea." *The Interpreter*, March 7, 2014. http://www.interpretermag.com/hackers-join-in-the-struggle-for-crimea/.

"Hacking Communities in the Deep Web." *InfoSec Institute*. Accessed July 22, 2015. http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/.

Halliday, Josh. "Stuxnet Worm Is the 'Work of a National Government Agency." *The Guardian*, September 24, 2010, sec. Technology. http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency.

Hauser, Kathryn. "Companies Hiring 'White Hat' Hackers To Expose Weaknesses." *CBS Boston*. Accessed September 9, 2015. http://boston.cbslocal.com/2014/10/20/companies-hiring-white-hat-hackers-to-expose-weaknesses/.

Headington, Yvonne. "A Lite On Niteworks." *BATTLESPACE News*, October 2013.

Heene, Aimé. *Bruggen Naar Het Onvoorspelbare: Theoretische Verkenningen En Een Stappenplan Voor Strategisch Leiderschap*. Tielt: Lannoo, 2015. http://www.literatuurplein.nl/boekdetail.jsp?boekId=1073588.

Heinzelman, Jessica, and Carol Waters. "Crowdsourcing Crisis Information in Disaster-Affected Haiti." Washington, DC: United States Institute of Peace, 2010. http://dspace.africaportal.org/jspui/bitstream/123456789/29753/1/Crowdsourcing%20Crisis%20Information%20in%20Disaster%20-%20Affected%20Haiti.pdf.

Hille, Kathrin. "Chinese Military Mobilises Cybermilitias." *Financial Times*, October 12, 2011. http://www.ft.com/intl/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz3hklhyqAp.

"I Am the Cavalry." *I Am the Cavalry*. Accessed September 10, 2015. https://www.iamthecavalry.org/.

InnoCentive. "InnoCentive Investigation of the Challenge Driven Innovation Platform at NASA." Public Report. Waltham, MA: InnoCentive, October 25, 2010. http://www.nasa.gov/pdf/572344main_InnoCentive_NASA_PublicReport_2011-0422.pdf.

"InnoCentive Challenge & Solver Statistics." *InnoCentive*, 2016. http://www.innocentive.com/about-innocentive/facts-stats.

"InnoCentive Idea Management." *InnoCentive*, 2015. http://www.innocentive.com/innovation-solutions/innocentive-idea-management.

"Innocentive Inc. in Andover, MA - Contracting Profile." *InsideGov*, 2015. http://government-contractors.insidegov.com/l/476/Innocentive-Inc-in-Andover-MA.

"Interface with RPDE Edition 3." RPDE, 2015.

"Interface with RPDE Edition 4." RPDE, 2015.

Joiner, Keith. "Implementing the Defence First Principles Review." Strategic Insights. Barton ACT, Australia: Australian Strategic Policy Institute, 2015. https://www.aspi.org.au/publications/implementing-the-defence-first-principles-review-two-key-opportunities-to-achieve-best-practice-in-capability-development/SI102_best_practice_capability_development.pdf.

Kausal, Tony, Stefan Markowski, and Defense Systems Management College, eds. *A Comparison of the Defense Acquisition Systems of France, United Kingdom, Germany and the United States*. Fort Belvoir, Va: Defense Systems Management College, 1999.

Keeton, Kathryn E., Elizabeth E. Richard, and C. J. Callini. "Collaboration Strategies within NASA: How to Accelerate Innovation." Galveston, TX, 2014. http://www.hou.usra.edu/meetings/hrp2014/pdf/3117.pdf.

Keeton, Kathryn E., Elizabeth E. Richard, and Jeffrey R. Davis. "Solution Mechanism Guide: Implementing Innovation Within a Research & Development Organization." *Aviation, Space, and Environmental Medicine* 85, no. 10 (October 1, 2014): 1061–62. doi:10.3357/ASEM.4050.2014.

"Klaar voor digitale strijd." Nieuwsbericht. *Defensie*, May 1, 2015. https://www.defensie.nl/actueel/nieuws/2015/05/01/klaar-voor-digitale-strijd.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (February 2011): 41–60. doi:10.1080/00396338.2011.555595.

Kurzweil, Ray. "The Singularity Is Near," 1999.

Lakhani, Karim R. "InnoCentive.com (A)," June 10, 2008. http://www.hbs.edu/faculty/Pages/item.aspx?num=36046.

Lakhani, Karin R., and Jill Panetta. "The Principles of Distributed Innovation." *Innovations* 2, no. 3 (Summer 2007): 97–112.

Landes, David S., Joel Mokyr, and William J. Baumol, eds. *The Invention of Enterprise: Entrepreneurship from Ancient Mesopotamia to Modern Times*. Princeton, N.J.: Princeton University Press, 2012.

Lee, Joel. "5 Of The World's Most Famous Hackers & What Happened To Them." *MakeUseOf*, June 1, 2012. http://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/.

Leson, Heather. "Deployments of the Week." *Ushahidi Wiki*, 2015. https://wiki.ushahidi.com/display/WIKI/Deployments+of+the+Week.

Levental, Simcha. "A New Geospatial Services Framework: How Disaster Preparedness Efforts Should Integrate Neogeography." *Journal of Map & Geography Libraries* 8, no. 2 (May 2012): 134–62. doi:10.1080/15420353.2012.670084.

Lifshitz-Assaf, Hila. "From Problem Solvers to Solution Seekers: Dismantling Knowledge Boundaries at NASA." SSRN Scholarly Paper. Social Science Research Network, April 1, 2015. http://papers.ssrn.com/abstract=2431717.

———. "From Problem Solvers to Solution Seekers: The Permeation of Knowledge Boundaries at NASA." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 4, 2015. http://papers.ssrn.com/abstract=2431717.

Lin, Albert. "Hacker/Prirate Interaction in the Computer Underground." MIT, 1995. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/lin-pirate.html.

Lucas S. Osborn. "Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms." Accessed August 27, 2015. http://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1096&context=fac_sw.

Mancini, Francesco, ed. "Big Data for Conflict Prevention: New Oil and Old Fires." In *New Technology and the Prevention of Violence and Conflict*, 4–27. New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013.

———. , ed. "Early Warning and the Role of New Technologies in Kenya." In *New Technology and the Prevention of Violence and Conflict*, 42–55. New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013.

———. , ed. "New Technologies and Conflict Prevention in Sudan and South Sudan." In *New Technology and the Prevention of Violence and Conflict*, 71–86. New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013.

———. , ed. "Using Information and Communication Technologies for Violence Prevention in Latin America." In *New Technology and the Prevention of Violence and Conflict*, 28–41. New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013.

Markoff, John. "Before the Gunfire, Cyberattacks." *The New York Times*, August 13, 2008, sec. Technology. http://www.nytimes.com/2008/08/13/technology/13cyber.html.

Martin, Adam. "The FBI Is Losing the War on Cybercrime." *The Wire*, June 6, 2011. http://www.theatlanticwire.com/technology/2011/06/fbi-losing-war-cyber-crime/38550/.

Maurer, Tim, and Scott Janz. "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context." *International Relations And Security Network*, October 17, 2014. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345.

Meier, Patrick. "Haiti: Taking Stock of How We Are Doing - Ushahidi." *Ushahidi*, February 7, 2010. http://www.ushahidi.com/blog/2010/02/07/haiti-taking-stock-of-how-we-are-doing.

———. "Haiti: Where We Are & Where We Go From Here - Ushahidi." *Ushahidi*, January 30, 2010. http://www.ushahidi.com/blog/2010/01/30/haiti-where-we-are-where-we-go-from-here.

———. "Introducing Ushahidi SWAT - Ushahidi." *Ushahidi*, August 1, 2011. http://www.ushahidi.com/blog/2011/08/01/introducing-ushahidi-swat/.

———. "Ushahidi & The Unprecedented Role of SMS in Disaster Response - Ushahidi." *Ushahidi*, February 23, 2010. http://www.ushahidi.com/blog/2010/02/23/ushahidi-the-unprecedented-role-of-sms-in-disaster-response.

———. "We Are The Volunteers of Mission 4636 - Ushahidi." *Ushahidi*, January 27, 2010. http://www.ushahidi.com/blog/2010/01/27/we-are-the-volunteers-of-mission-4636.

Mora, F. A. "Innovating in the Midst of Crisis: A Case Study of Ushahidi." *Submitted for Publication to SAGE Convergence Journal*, 2011. http://www.researchgate.net/profile/Fernando_Mora3/publication/231537244_Innovating_in_the_midst_of_crisis_A_case_study_of_Ushahidi/links/0fcfd506b9fdd4086b000000.pdf.

Morrow, Nathan, Nancy Mock, Adam Papendieck, and Nicholas Kocmich. "Independent Evaluation of the Ushahidi Haiti Project." Development Information Systems International, 2011. http://ggs684.pbworks.com/w/file/fetch/60819963/1282.pdf.

Munro, Robert. "Crowdsourced Translation for Emergency Response in Haiti: The Global Collaboration of Local Knowledge." In *AMTA Workshop on Collaborative Crowdsourcing for Translation*, 1–4, 2010. http://jan.stanford.edu/pubs/munro2010translation.pdf.

———. "Crowdsourcing and the Crisis-Affected Community: Lessons Learned and Looking Forward from Mission 4636." *Inf Retrieval Information Retrieval* 16, no. 2 (2013): 210–66.

Nakashima, Ellen, and Joby Warrick. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." *The Washington Post*, June 1, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U_story.html.

"NASA Touts Successes Of Centennial Challenges | AWIN Content from Aviation Week." *Aviationweek*, March 4, 2013. http://aviationweek.com/awin/nasa-touts-successes-centennial-challenges.

Nelson, Richard R. *Technology, Institutions, and Economic Growth*. Harvard University Press, 2005.

Niteworks. "Army Equipment Development Plan (AEDP)." Niteworks, 2011. http://www.niteworks.net/workspace/website-files/army-equipment-development-plan.pdf.

———. "General Information and Documentation from Niteworks," 2015. http://www.niteworks.net/general-information-and-documents/.

"Niteworks Contract Extended to 2018 | MOD-DCO." *MoD*, September 14, 2015. https://www.contracts.mod.uk/blog/niteworks-contract-extended-to-2018/.

Oduor Lungati, Angela. "Connecting Digital Networks to Strengthen Electoral Processes: A NEW SIGN OF HOPE." *Ushahidi*, April 24, 2015. http://www.ushahidi.com/blog/2015/04/24/connecting-digital-networks-to-strengthen-electoral-processes-a-new-sign-of-hope.

Okolloh, Ory. "Ushahidi, Or'testimony': Web 2.0 Tools for Crowdsourcing Crisis Information." *Participatory Learning and Action* 59, no. 1 (2009): 65–70.

"One in Four US Hackers 'Is an FBI Informer' | Technology | The Guardian." Accessed September 14, 2015. http://www.theguardian.com/technology/2011/jun/06/us-hackers-fbi-informer.

"Open Street Map Community Responds to Haiti Crisis." *Open Knowledge Blog*, January 15, 2010. http://blog.okfn.org/2010/01/15/open-street-map-community-responds-to-haiti-crisis/.

Ottis, Rain. "Theoretical Offensive Cyber Militia Models." In *Leading Issues in Information Warfare and Security Research*, by Julie J. C. H. Ryan, 131–44. Reading: Academic Publishing International Ltd., 2011.

Perez, Carlota. *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*. Cheltenham UK; Northampton MA USA: Edward Elgar Publishing, 2002.

Phillips, Veronica. "Open Government at NASA." Text. *NASA*, March 3, 2015. http://www.nasa.gov/open/plan.

Pilkington, Ed. "LulzSec Hacker 'Sabu' Released after 'Extraordinary' FBI Cooperation." *The Guardian*, May 27, 2014, sec. Technology. http://www.theguardian.com/technology/2014/may/27/hacker-sabu-walks-free-sentenced-time-served.

Pisano, Gary P., and Roberto Verganti. "Which Kind of Collaboration Is Right for You?" *Harvard Business Review* 86, no. 12 (December 2008): 78–86.

Polityuk, Pavel, and Jim Finkle. "Ukraine Says Communications Hit, MPs Phones Blocked." *Reuters*, March 4, 2014. http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.

Posey, Brien. "Hiring Hackers As Security Consultants." *WindowSecurity.com*. Accessed September 15, 2015. http://www.windowsecurity.com/articles-tutorials/misc_network_security/Hackers-Security-Consultants.html.

Purcell, Ian. "Tasking Niteworks – A Guide for MOD Staff." Niteworks, 2012.

RAND Corporation. "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Review of U.S. Human Spaceflight Plans Committee. "Seeking a Human Spaceflight Program Worthy of a Great Nation." NASA, October 2009. http://www.nasa.gov/pdf/617036main_396093main_HSF_Cmte_FinalReport.pdf.

Richard, Elizabeth E., and Jeffrey R. Davis. "NASA Space Life Sciences Strategy for Human Space Exploration." NASA, May 2007.

Richard, Elizabeth E., and Steven A. González. "Strategic Alliances Strategies and Processes Benchmarking Study." Benchmark Study. NASA, June 2009. http://www.nasa.gov/sites/default/files/atoms/files/strategic_alliances_strategies_and_processes_benchmarking_study_2009.pdf.

Roberts, Shadrock. "Supporting Online Volunteer Response to the Nepal Earthquake - Ushahidi." *Ushahidi*, April 25, 2015. http://www.ushahidi.com/blog/2015/04/25/supporting-online-volunteer-response-to-the-nepal-earthquake.

Roberts, Shadrock, and Karen Payne. "Operationalizing VGI for Humanitarian Response: Is It Possible and What Does It Mean." In *Association of American Geographers Conference on Volunteered Geographic Information*, 2011. http://vgi.spatial.ucsb.edu/sites/vgi.spatial.ucsb.edu/files/file/aag/Roberts_abstract.pdf.

Roco, Mihail C., and William Sims Bainbridge, eds. *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. Dordrecht ; Boston, Mass: Kluwer Academic Publishers, 2003.

Roco, Mihail C., William Bainbridge, Bruce Tonn, and George Whitesides. *Convergence of Knowledge, Technology and Society: Beyond Convergence of Nano-Bio-Info-Cognitive Technologies*. Springer Science & Business Media, 2014.

RPDE. "Strategic Plan 2014–2016." Rapid Prototyping Development and Evaluation Program, November 19, 2013. https://www.rpde.org.au/publications/1/file/p18g4pgo7i1c73uaq1ujhq0vo121.

"RPDE - About Us." *RPDE*, 2016. http://www.rpde.org.au/about.

Ruffer, Galya B. "What Ushahidi Can Do to Track Displacement." *Forced Migration Review*, no. 38 (oktober 2011): 25–26.

Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia." *The European Institute*, Winter/Spring 2008. http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Sara Yin. "7 Hackers Who Got Legit Jobs From Their Exploits." *PCMAG*, June 2011. http://www.pcmag.com/slideshow/story/266255/7-hackers-who-got-legit-jobs-from-their-exploits.

Schultz, Friederike, Sonja Utz, and Anja Göritz. "Is the Medium the Message? Perceptions of and Reactions to Crisis Communication via Twitter, Blogs and Traditional Media." *Public Relations Review Public Relations Review* 37, no. 1 (2011): 20–27.

Schwartz, Moshe. "Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process." Congressional Research Service, 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA520832.

Scott D. Applegate. "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations," 2012. https://www.academia.edu/1261902/Leveraging_Cyber_Militias_as_a_Force_Multiplier_in_Cyber_Operations.

Scott Tompson. "Tight vs. Loose Coupling Organizational Structure." Demand Media. *Small Business - Chron.com*. Accessed August 27, 2015. http://smallbusiness.chron.com/tight-vs-loose-coupling-organizational-structure-69016.html.

Security.nl. "UWV: Tekort Aan Hoogopgeleide Security-Specialisten," September 11, 2015. https://www.security.nl/posting/443041/UWV%3A+tekort+aan+hoogopgeleide+security-specialisten.

Semon, Ted. "Results from the 2010 Strong Tether Challenge." *The Space Elevator Blog*, August 13, 2010. http://www.spaceelevatorblog.com/?p=1420.

Shepard, Sophie. "Designing the Front-End of Ushahidi V3 - Ushahidi." *Ushahidi*, February 25, 2015. http://www.ushahidi.com/blog/2015/02/25/designing-the-front-end-of-ushahidi-v3.

Shephard News Team. "UK MoD Extends Niteworks to 2018 - News - Shephard," August 28, 2015. http://www.shephardmedia.com/news/digital-battlespace/uk-mod-extends-niteworks-2018/.

Smith, Gerry. "Feds Turn To Hackers To Defend Nation in Cyberspace." *The Huffington Post*, August 8, 2011. http://www.huffingtonpost.com/2011/08/08/government-recruits-hackers-cyber-shortage_n_920795.html.

Spandana, Vidya. "Bittersweet Farewell to SwiftRiver - Ushahidi." *Ushahidi*, December 8, 2014. http://www.ushahidi.com/blog/2014/12/08/bittersweet-farewell-swiftriver.

Spradlin, Dwayne. "InnoCentive Oil Spill Challenge - BP's Response." *InnoCentive Blog*, June 23, 2010. http://www.innocentive.com/blog/2010/06/23/innocentive-oil-spill-challenge-bps-response/.

Stephen Foley. "Facebook Hires Hacker Who Started Sony War," June 29, 2011. http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-hires-hacker-who-started-sony-war-2304075.html.

Stinson, Liz. "How GE Plans to Act Like a Startup and Crowdsource Breakthrough Ideas." *WIRED*, April 11, 2014. http://www.wired.com/2014/04/how-ge-plans-to-act-like-a-startup-and-crowdsource-great-ideas/.

Stoetzel, Martin, Martin Wiener, and Michael Amberg. "Key Differentiators of Open Innovation Platforms–a Market-Oriented Perspective." In *Wirtschaftinformatik Proceedings 2011*. Zurich, Switzerland, 2011.

"Student Initiatives." *The Fletcher School | Tufts University*. Accessed September 15, 2015. http://fletcher.tufts.edu/Hitachi/Student-Initiatives.

Suehr, Debbie. "InnoCentive." Adapted Privacy Impact Assessment. Department of Homeland Security, July 24, 2015. https://www.doi.gov/sites/doi.opengov.ibmcloud.com/files/uploads/Innocentive-Adapted-PIA.pdf.

Tapscott, Don. "Introducing Global Solution Networks: Understanding the New Multi-Stakeholder Models for Global Cooperation, Problem Solving and Governance." *Innovations* 9, no. 1–2 (2014): 3–46.

———. *The Digital Economy ANNIVERSARY EDITION: Rethinking Promise and Peril in the Age of Networked Intelligence*. 2 edition. New York: McGraw-Hill Education, 2014.

———. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. McGraw-Hill, 1996.

———. "The Era of Global Solution Networks." *Rotman Management*, Fall 2014, 54–59.

Tapscott, Don, and Anthony D. Williams. *Wikinomics: How Mass Collaboration Changes Everything*. Penguin, 2008.

TEDGlobal 2011. *Hire the Hackers!* Accessed August 3, 2015. https://www.ted.com/talks/misha_glenny_hire_the_hackers.

"Terms of Use (Seeker)." *InnoCentive*, 2012. http://www.innocentive.com/brain/terms.

"The United States Cyber Challenge - The United States Cyber Challenge 1.1 (updated 5-8-09)." Accessed August 3, 2015. https://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20(updated%205-8-09).pdf.

Thompson, Derek. "Finding the Next Edison - The Atlantic," January 2014. http://www.theatlantic.com/magazine/archive/2014/01/finding-the-next-edison/355747/.

Thompson, Victor A. "Bureaucracy and Innovation." *Administrative Science Quarterly* 10, no. 1 (June 1, 1965): 1–20. doi:10.2307/2391646.

UK House of Commons Committee of Public Accounts. *Ministry of Defence: Major Projects Report 2007: Report, Together with Formal Minutes, Oral and Written Evidence*. London: TSO, 2008.

Unabor, H. "Geospatial Response with Remote Sensing, GIS, OpenStreetMap and Ushahidi: The Haiti Eartchquake of 12th Januarry, 2010." *International Journal of Scientific & Engineering Research* 5, no. 2 (February 2014). http://www.ijser.org/paper/Geospatial-Response-with-Remote-Sensing-GIS-OpenStreetMap.html.

"U.N. General Assembly Condemns Russia's Actions in Ukraine - CBS News." Accessed September 3, 2015. http://www.cbsnews.com/news/un-general-assembly-condemns-russias-actions-in-ukraine/.

United Nations Foundation, Vodafone Foundation, Harvard Humanitarian Initiative, United Nations, and Office for the Coordination of Humanitarian Affairs. *Disaster Relief 2.0 the Future of Information Sharing in Humanitarian Emergencies.* Washington, D.C.; Berkshire, UK: UN Foundation & Vodafone Foundation Technology Partnership, 2011. http://www.globalproblems-globalsolutions-files.org/gpgs_files/pdf/2011/DisasterResponse.pdf.

"U.S Defense Giants Are Hiring the Best Hackers They Can Find (with a Few Caveats) | VentureBeat | Security | by Richard Byrne Reilly." Accessed September 14, 2015. http://venturebeat.com/2014/08/11/u-s-defense-giants-are-hiring-the-best-hackers-they-can-find-with-a-few-caveats/.

Vericat, Jose. "Open Source Mapping as Liberation Technology: An Interview with David Kobia." *Journal of International Affairs* 64, no. 1 (2010): 195.

Von Hippel, Eric. *Democratizing Innovation*, 2005. http://web.mit.edu/evhippel/www/democ1.htm.

Voordouw, Jan. "Question about Haiti Relief Effort and Cooperation," September 12, 2015.

Wachanga, D Ndirangu. "Participatory Culture in an Emerging Information Ecosystem: Lessons from Ushahidi." *Communicatio* 38, no. 2 (August 2012): 195–212. doi:10.1080/02500167.2012.717348.

Were, Daudi. "Ushahidi Version 3.0 Is Here - Ushahidi." *Ushahidi*, August 19, 2015. http://www.ushahidi.com/blog/2015/08/19/ushahidi-version-3-0-is-here.

Wiggins, Robert R., and Timothy W. Ruefli. "Sustained Competitive Advantage: Temporal Dynamics and the Incidence and Persistence of Superior Economic Performance." *Organization Science* 13, no. 1 (January 2002): 81–105. doi:10.1287/orsc.13.1.81.542.

Wilkinson, Dennis, and Bernardo Huberman. "Cooperation and Quality in Wikipedia," no. WikiSym'07, October 21–23, 2007, Montr´eal, Qu´ebec, Canada. (October 2007). https://www.researchgate.net/publication/200772402_Cooperation_and_quality_in_Wikipedia.

Williams, Matthew. "The NASA Centennial Challenge Program," December 19, 2014. https://herox.com/news/150-the-nasa-centennial-challenge-program.

Wong, Sterling. "Hackers Linked to China's Army Seen From EU to D.C." *Bloomberg.com*, July 27, 2012. http://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *WIRED*, November 3, 2014. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zhan, Liuhan, Nan Wang, Shen Xiao-Liang, and Sun Yongqiang. "Knowledge Quality of Collaborative Editing in Wikipedia: An Integrative Perspective of Social Capital and Team Conflict." Accessed January 22, 2016. http://pacis2015.comp.nus.edu.sg/_proceedings/PACIS_2015_submission_245.pdf.

ENDNOTES

ENDNOTES

1. Dennis Wilkinson and Bernardo Huberman, "Cooperation and Quality in Wikipedia," no. WikiSym'07, October 21–23, 2007, Montr´eal, Qu´ebec, Canada. (October 2007), https://www.researchgate.net/publication/200772402_Cooperation_and_quality_in_Wikipedia.
2. Liuhan Zhan et al., "Knowledge Quality of Collaborative Editing in Wikipedia: An Integrative Perspective of Social Capital and Team Conflict," accessed January 22, 2016, http://pacis2015.comp.nus.edu.sg/_proceedings/PACIS_2015_submission_245.pdf.
3. Clingendael and HCSS, " Internationale Materieelsamenwerking. Rapport ten behoeve van het Interdepartementaal Beleidsonderzoek (IBO) naar internationale samenwerking op het gebied van defensiematerieel", Janury 2015, bijlage 3 and 4.
4. Readers interested in reading up more on these issues may find the following works interesting: Eric Beinhocker, *The Origin of Wealth: Evolution, Complexity, and the Radical Remaking of Economics* (Boston Mass.: Harvard Business School Press, 2006); Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture* (Amsterdam; Boston: Morgan Kaufmann/Elsevier, 2011); Aimé Heene, *Bruggen Naar Het Onvoorspelbare: Theoretische Verkenningen En Een Stappenplan Voor Strategisch Leiderschap* (Tielt: Lannoo, 2015), http://www.literatuurplein.nl/boekdetail.jsp?boekId=1073588.
5. That part of the defense planning community that focuses on tomorrow rather than on today. The tomorrow time horizon is currently still frequently defined as 15-20-30 years ahead, but it is becoming increasingly clear that in periods of rapid change like today, it might as well be 2-3 years from now. In our view, the key element here is not time per se (about which we know depressingly little) but the degree of (in)visibility of risk and uncertainty.
6. We refer here to our observation that most acquisition processes deal with weapon systems or platforms, and not with military (or defense) capabilities as we have defined it. See Stephan De Spiegeleire, "Ten Trends in Capability Planning for Defence and Security," The RUSI Journal 156, no. 5 (October 1, 2011): 20–28, doi:10.1080/03071847.2011.626270.
7. Stephan de Spiegeleire and Tim Sweijs, "Missile Defense – An Interactive Policy Analysis," HCSS Centre for Strategic Studies, July 11, 2011, http://www.hcss.nl/news/missile-threats-against-the-netherlands/309/; Stephan de Spiegeleire and Eline Chivot, "Assessing Assertions of Assertiveness: The Chinese and Russian Cases – Reports," HCSS Centre for Strategic Studies, June 3, 2014, http://www.hcss.nl/reports/assessing-assertions-of-assertiveness-the-chinese-and-russian-cases/145/.
8. GitHub · Build Software Better, Together," accessed August 27, 2015, https://github.com/.

9. For example Lucas S. Osborn, "Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms," accessed August 27, 2015, http://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1096&context=fac_sw.
10. Scott Tompson, "Tight vs. Loose Coupling Organizational Structure," Demand Media, *Small Business – Chron.com*, accessed August 27, 2015, http://smallbusiness.chron.com/tight-vs-loose-coupling-organizational-structure-69016.html.
11. "Defensie en Thales onderhouden samen luchtruimverdedigings-systemen," Defensie, April 22, 2015, https://www.defensie.nl/actueel/nieuws/2015/04/22/defensie-en-thales-onderhouden-samen-luchtruimverdediging.
12. Liz Stinson, "How GE Plans to Act Like a Startup and Crowdsource Breakthrough Ideas," WIRED, April 11, 2014, http://www.wired.com/2014/04/how-ge-plans-to-act-like-a-startup-and-crowdsource-great-ideas/.
13. Victor A. Thompson, "Bureaucracy and Innovation," *Administrative Science Quarterly* 10, no. 1 (June 1, 1965): 1–20, doi:10.2307/2391646.
14. Anahita Baregheh, Jennifer Rowley, and Sally Sambrook, "Towards a Multidisciplinary Definition of Innovation," *Management Decision* 47, no. 8 (September 4, 2009): 1323–39, doi:10.1108/00251740910984578.
15. "About Open Innovation," *EIDON Lab*, October 10, 2011, http://www.eidon-lab.eu/index/index.php?option=com_content&view=article&id=66&lang=en.
16. Ibid.
17. See for example a book by Eric Von Hippel "Democratizing Innovation" (2005) that focuses on the importance of user innovation. It is posted under a Creative Commons license free of charge to the public at: Eric Von Hippel, *Democratizing Innovation*, 2005, http://web.mit.edu/evhippel/www/democ1.htm. and as such can be considered as an example of the trend toward more open innovation.
18. "About Open Innovation."
19. Karin R. Lakhani and Jill Panetta, "The Principles of Distributed Innovation," *Innovations* 2, no. 3 (Summer 2007): 97–112.
20. Henry W. Chesbrough, "The Era of Open Innovation," *MIT Sloan Management Review*, Spring 2003.
21. See Wetenschappelijke Raad voor het Regeringsbeleid, *Naar een lerende economie*, November 2013.
22. Gary P. Pisano and Roberto Verganti, "Which Kind of Collaboration Is Right for You?," *Harvard Business Review* 86, no. 12 (December 2008): 78–86.
23. Ibid.
24. Martin Stoetzel, Martin Wiener, and Michael Amberg, "Key Differentiators of Open Innovation Platforms–a Market-Oriented Perspective," in *Wirtschaftinformatik Proceedings 2011* (10th International Conference on Wirtschaftinformatik, Zurich, Switzerland, 2011).
25. Ibid.
26. "InnoCentive Challenge & Solver Statistics," *InnoCentive*, 2016, http://www.innocentive.com/about-innocentive/facts-stats.
27. Robert R. Wiggins and Timothy W. Ruefli, "Sustained Competitive Advantage: Temporal Dynamics and the Incidence and Persistence of Superior Economic Performance," *Organization Science* 13, no. 1 (January 2002): 81–105, doi:10.1287/orsc.13.1.81.542.
28. Derek Thompson, "Finding the Next Edison – The Atlantic," January 2014, http://www.theatlantic.com/magazine/archive/2014/01/finding-the-next-edison/355747/.
29. Karim R. Lakhani, "InnoCentive.com (A)," June 10, 2008, http://www.hbs.edu/faculty/Pages/item.aspx?num=36046.

30. Solvers can choose to solve challenges individually or join a team. By joining a team all team members submit one solution, choose a team leader and decide how to share the prize in case of winning the challenge.
31. "Frequently Asked Questions," *InnoCentive*, 2015, http://www.innocentive.com/faq/Solver.
32. Ibid.
33. "Terms of Use (Seeker)," *InnoCentive*, 2012, http://www.innocentive.com/brain/terms.
34. "Frequently Asked Questions," *InnoCentive*, 2015, http://www.innocentive.com/faq/Solver.
35. "Terms of Use (Seeker)."
36. "Frequently Asked Questions," 2015.
37. "Challenge Specific Agreement," *InnoCentive*, accessed October 2, 2015, https://www.innocentive.com/ar/contract/printUnsigned/36.
38. Ibid.
39. Ibid.
40. "Frequently Asked Questions," 2015.
41. "InnoCentive Idea Management," *InnoCentive*, 2015, http://www.innocentive.com/innovation-solutions/innocentive-idea-management.
42. Thomas Franklin, "Home Phe Monitor Research Challenge Advancing the Treatment for PKU," 2013, http://npkua.org/Portals/0/PDFs/2014Conference/Home%20Phe%20Monitor%20Dr%20Tom%20Franklin.pdf.
43. A 2014 Tufts study (see http://csdd.tufts.edu/news/complete_story/pr_tufts_csdd_2014_cost_study) estimated that in the pharmaceutical industry the costs associated with developing a prescription medicine and getting market approval is $2.558 billion on average ($1.395 billion average out-of-pocket costs and $1.163 billion time costs). This also includes the cost of failures. In the automotive industry, R&D costs per vehicle is $1,200 on average. The US spends $18 billion out of the $100 billion spent annually on R&D in the automotive industry. See http://www.autoalliance.org/auto-innovation/2014-car-report
44. Michelle Bishop, "The Total Economic Impact Of InnoCentive Challenges: Single Company Case Study" (Forrester Comsulting, January 5, 2009), https://www.innocentive.com/files/node/casestudy/total-economic-impacttm-innocentive-challenges-sca-case-study.pdf.
45. Hila Lifshitz-Assaf, "From Problem Solvers to Solution Seekers: Dismantling Knowledge Boundaries at NASA," SSRN Scholarly Paper (Social Science Research Network, April 1, 2015), http://papers.ssrn.com/abstract=2431717.
46. Jeffrey R. Davis, Elizabeth E. Richard, and Kathryn E. Keeton, "Open Innovation at NASA: A New Business Model for Advancing Human Health and Performance Innovations," *Research-Technology Management* 58, no. 3 (May 1, 2015): 52–58, doi:10.5437/08956308X5803325.
47. Kathryn E. Keeton, Elizabeth E. Richard, and Jeffrey R. Davis, "Solution Mechanism Guide: Implementing Innovation Within a Research & Development Organization," *Aviation, Space, and Environmental Medicine* 85, no. 10 (October 1, 2014): 1061–62, doi:10.3357/ASEM.4050.2014. Kathryn E. Keeton, Elizabeth E. Richard, and C. J. Callini, "Collaboration Strategies within NASA: How to Accelerate Innovation" (NASA Human Research Program Investigators' Workshop, Galveston, TX, 2014), http://www.hou.usra.edu/meetings/hrp2014/pdf/3117.pdf.
48. Keeton, Richard, and Davis, "Solution Mechanism Guide." Keeton, Richard, and Callini, "Collaboration Strategies within NASA: How to Accelerate Innovation."
49. Bernard Gray, "Review of Acquisition for the Secretary of State for Defence: An Independent Report by Bernard Gray" (Ministry of Defence of the UK, 2009); Moshe Schwartz, "Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process" (Congressional Research Service, 2010), http://oai.dtic.mil/

oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA520832; Andrew Davies, Peter Jennings, and Mark Thomson, "One Defence: One Direction? The First Principles Review of Defence," Special Report (Barton ACT, Australia: Australian Strategic Policy Institute, 2015); Department of Defence, Australia, *First Principles Review: Creating One Defence* (Canberra, Australian Capital Territory: Department of Defence, 2015), http://apo.org.au/research/first-principles-review-creating-one-defence; Keith Joiner, "Implementing the Defence First Principles Review," Strategic Insights (Barton ACT, Australia: Australian Strategic Policy Institute, 2015), https://www.aspi.org.au/publications/implementing-the-defence-first-principles-review-two-key-opportunities-to-achieve-best-practice-in-capability-development/SI102_best_practice_capability_development.pdf; Tony Kausal, Stefan Markowski, and Defense Systems Management College, eds., *A Comparison of the Defense Acquisition Systems of France, United Kingdom, Germany and the United States* (Fort Belvoir, Va: Defense Systems Management College, 1999); Jacques S. Gansler and William Lucyshyn, "Reforming Acquisition: This Time Must Be Different," in *Proceedings of the Twelfth Annual Acquisition Research Symposium* (Twelfth Annual Acquisition Research Symposium, College Park, MD: Maryland Univ College Park Center for Public Policy and Private Enterprise, 2015); Jason R. Gerard, "Defense Acquisition Reform: A Half-Century and Still Counting" (Army Command and General Staff College, 2014); "British Defence-Acquisition Reform – The RUSI Journal – Volume 159, Issue 1," accessed January 24, 2016, http://www.tandfonline.com/doi/abs/10.1080/03071847.2014.895256#.VqVFKIltAhM.

50. In some countries with a smaller national defense industry, for instance, this process was more insulated from such commercial pressures than in countries with more powerful defense industrial players.
51. De Spiegeleire, "Ten Trends in Capability Planning for Defence and Security."
52. "There is a 'conspiracy of optimism' in the project teams and industry which also extends to the leadership of the Department, who often appear willing to accept an estimate that is the nearest match to the available resources. There is a perception that equipment can be brought into service at a lower price, but with little hard evidence to support such an assumption". UK House of Commons Committee of Public Accounts, *Ministry of Defence: Major Projects Report 2007: Report, Together with Formal Minutes, Oral and Written Evidence* (London: TSO, 2008), 14.
53. Witness also its (failed) attempt to outsource its entire acquisition process to a government owned, contractor operated entity.
54. "Defence Industrial Strategy" (UK Ministry of Defence, December 2005), 127.
55. Niteworks, "General Information and Documentation from Niteworks," 2015, http://www.niteworks.net/general-information-and-documents/.
56. Shephard News Team, "UK MoD Extends Niteworks to 2018 – News – Shephard," August 28, 2015, http://www.shephardmedia.com/news/digital-battlespace/uk-mod-extends-niteworks-2018/.
57. Ian Purcell, "Tasking Niteworks – A Guide for MOD Staff" (Niteworks, 2012).
58. Sponsors are MOD employees seeking a solution to a specific problem or challenge
59. Yvonne Headington, "A Lite On Niteworks," *BATTLESPACE News*, October 2013.
60. Ibid.
61. "Equipping the Army for the Future," *MooD Smarter Decisions*, accessed January 28, 2016, http://www.moodinternational.com/casestudies_niteworks.html.
62. Niteworks, "Army Equipment Development Plan (AEDP)" (Niteworks, 2011), http://www.niteworks.net/workspace/website-files/army-equipment-development-plan.pdf.
63. Jessie-May Brown and Pincher Martin, "Talon Strike – Securing a Clear View of the Battlefield," *Royal United Services Institute*, 2011.

64. Ibid.
65. Ibid.
66. Ibid. Bob Barton and Dick Whittington, "Meeting Capability Goals through Effective Modelling and Experimentation of C4ISTAR Options," June 2011, http://www.dodccrp.org/events/16th_iccrts_2011/presentations/007.pdf.
67. Headington, "A Lite On Niteworks."
68. "Niteworks Contract Extended to 2018 | MOD-DCO," *MoD*, September 14, 2015, https://www.contracts.mod.uk/blog/niteworks-contract-extended-to-2018/.
69. "RPDE – About Us," *RPDE*, 2016, http://www.rpde.org.au/about.
70. RPDE, "Strategic Plan 2014–2016" (Rapid Prototyping Development and Evaluation Program, November 19, 2013), 5, https://www.rpde.org.au/publications/1/file/p18g4pgo7i1c73uaq1ujhq0vo121.
71. "Interface with RPDE Edition 4" (RPDE, 2015).
72. "Interface with RPDE Edition 3" (RPDE, 2015), 3.
73. Veronica Phillips, "Open Government at NASA," Text, *NASA*, (March 3, 2015), http://www.nasa.gov/open/plan.
74. Ibid.
75. Frank Gaglioti, "Cuts to NASA Budget Gut Space Research – World Socialist Web Site," *World Socialist Web Site*, May 20, 2006, https://www.wsws.org/en/articles/2006/05/nasa-m20.html.
76. Elizabeth E. Richard and Jeffrey R. Davis, "NASA Space Life Sciences Strategy for Human Space Exploration" (NASA, May 2007).
77. Review of U.S. Human Spaceflight Plans Committee, "Seeking a Human Spaceflight Program Worthy of a Great Nation" (NASA, October 2009), http://www.nasa.gov/pdf/617036main_396093main_HSF_Cmte_FinalReport.pdf.
78. Elizabeth E. Richard and Steven A. González, "Strategic Alliances Strategies and Processes Benchmarking Study," Benchmark Study (NASA, June 2009), http://www.nasa.gov/sites/default/files/atoms/files/strategic_alliances_strategies_and_processes_benchmarking_study_2009.pdf.
79. Richard and Davis, "NASA Space Life Sciences Strategy for Human Space Exploration."
80. Davis, Richard, and Keeton, "Open Innovation at NASA."
81. InnoCentive, "InnoCentive Investigation of the Challenge Driven Innovation Platform at NASA," Public Report (Waltham, MA: InnoCentive, October 25, 2010), http://www.nasa.gov/pdf/572344main_InnoCentive_NASA_PublicReport_2011-0422.pdf. Davis, Richard, and Keeton, "Open Innovation at NASA."
82. Davis, Richard, and Keeton, "Open Innovation at NASA."
83. Matthew Williams, "The NASA Centennial Challenge Program," December 19, 2014, https://herox.com/news/150-the-nasa-centennial-challenge-program.
84. Ted Semon, "Results from the 2010 Strong Tether Challenge," *The Space Elevator Blog*, August 13, 2010, http://www.spaceelevatorblog.com/?p=1420.
85. "NASA Touts Successes Of Centennial Challenges | AWIN Content from Aviation Week," *Aviationweek*, March 4, 2013, http://aviationweek.com/awin/nasa-touts-successes-centennial-challenges.
86. Hila Lifshitz-Assaf, "From Problem Solvers to Solution Seekers: The Permeation of Knowledge Boundaries at NASA," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 4, 2015), http://papers.ssrn.com/abstract=2431717.
87. In fact, this is rapidly becoming a big issue in the corporate world as well, putting constraints on open innovation in many civil sectors.

88. See also Strategische Kennis & Innovatieagenda 2015 (forthcoming).
89. It should be noted that, in terms of defense capabilities, this is an example at component or subsystem level. Other examples of open 'business solutions' may better illustrate the possibilities at system of systems level, equivalent to the level of main weapon platforms or even more integrate capabilities such as task forces.
90. Davis, Richard, and Keeton, "Open Innovation at NASA."
91. "Innocentive Inc. in Andover, MA – Contracting Profile," *InsideGov*, 2015, http://government-contractors.insidegov.com/l/476/Innocentive-Inc-in-Andover-MA.
92. Debbie Suehr, "InnoCentive," Adapted Privacy Impact Assessment (Department of Homeland Security, July 24, 2015), https://www.doi.gov/sites/doi.opengov.ibmcloud.com/files/uploads/Innocentive-Adapted-PIA.pdf.
93. Bureau of Public Affairs Department Of State. The Office of Website Management, "Morocco," Report (Department Of State. The Office of Website Management, Bureau of Public Affairs., June 8, 2012), moroccol, http://www.state.gov/e/eb/rls/othr/ics/2012/191203.htm.
94. "$1 Million Prize Awarded for New Algorithm for Rapid Characterization of Pathogens," *InnoCentive*, March 12, 2013, http://www.innocentive.com/1-million-prize-awarded-new-algorithm-rapid-characterization-pathogens.
95. "CTTSO Challenge: Pre-Event Insider Attack Recognition," *InnoCentive*, 2014, https://www.innocentive.com/ar/challenge/9933546.
96. Dwayne Spradlin, "InnoCentive Oil Spill Challenge – BP's Response," *InnoCentive Blog*, June 23, 2010, http://www.innocentive.com/blog/2010/06/23/innocentive-oil-spill-challenge-bps-response/.
97. Frank S. Grevil, "Gauging Sympathy for Snowden," *Consortiumnews*, July 3, 2013, https://consortiumnews.com/2013/07/03/gauging-sympathy-for-snowden/.
98. "U.N. General Assembly Condemns Russia's Actions in Ukraine – CBS News," accessed September 3, 2015, http://www.cbsnews.com/news/un-general-assembly-condemns-russias-actions-in-ukraine/.
99. "I Am the Cavalry," *I Am the Cavalry*, accessed September 10, 2015, https://www.iamthecavalry.org/.
100. Kathryn Hauser, "Companies Hiring 'White Hat' Hackers To Expose Weaknesses," *CBS Boston*, accessed September 9, 2015, http://boston.cbslocal.com/2014/10/20/companies-hiring-white-hat-hackers-to-expose-weaknesses/.
101. Joel Lee, "5 Of The World's Most Famous Hackers & What Happened To Them," *MakeUseOf*, June 1, 2012, http://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/.
102. Albert Lin, "Hacker/Prirate Interaction in the Computer Underground" (MIT, 1995), http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/lin-pirate.html.
103. Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *The European Institute*, Winter/Spring 2008, http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.
104. Cristen Conger, "Could a Single Hacker Crash a Country's Network? – Estonia's Hack Attack," *HowStuffWorks*, accessed September 9, 2015, http://computer.howstuffworks.com/hacker-crash-country-network.htm.
105. RAND Corporation, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
106. E. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London ; New York: Verso, 2014).
107. David Gilbert, "Ashley Madison Hack: Who Are Impact Team, Why Did They Leak Website Data and Will They Be Caught?," *International Business Times*, August 2015, http://www.ibtimes.co.uk/ashley-madison-hack-who-are-impact-team-why-did-they-leak-website-data-will-they-be-caught-1516328.

108. One illustration of this warning comes from the story of Ross Ulbricht, the founder of an online black market called Silk Road. He hired a hitman to punish a Silk Road staffer who was suspected of stealing Bitcoins and paid $80,000 to the killer when he received fake pictures of the man being tortured and subsequently killed. Unfortunately for Ulbricht, the hired hitman was an undercover government agent and the murder never happened. See also: Nick Allen, "Hit Men, Drugs and the Fall of Ross Ulbricht, the Silk Road 'Mastermind,'" *The Telegraph*, October 4, 2013, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10356444/Hit-men-drugs-and-the-fall-of-Ross-Ulbricht-the-Silk-Road-mastermind.html.
109. TEDGlobal 2011, *Hire the Hackers!*, accessed August 3, 2015, https://www.ted.com/talks/misha_glenny_hire_the_hackers.
110. RAND Corporation, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar."
111. "Hacking Communities in the Deep Web," *InfoSec Institute*, accessed July 22, 2015, http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/.
112. Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 7.
113. Trolling is an activity that seeks to desecrate the reputations of individuals and organizations, by revealing embarrassing and personal information.
114. The Church of Scientology is an organization devoted to the practice, administration and dissemination of Scientology, a new religious movement.
115. Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 3.
116. Coleman, *Hacker, Hoaxer, Whistleblower, Spy*.
117. John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 13, 2008, sec. Technology, http://www.nytimes.com/2008/08/13/technology/13cyber.html.
118. Dancho Danchev, "Georgia President's Web Site under DDoS Attack from Russian Hackers," *ZDNet*, July 22, 2008, http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/.
119. Markoff, "Before the Gunfire, Cyberattacks."
120. Danchev, "Georgia President's Web Site under DDoS Attack from Russian Hackers."
121. Sterling Wong, "Hackers Linked to China's Army Seen From EU to D.C.," *Bloomberg.com*, July 27, 2012, http://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.
122. Mark Clayton, "Stealing US Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China," *Christian Science Monitor*, September 14, 2012, http://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China.
123. Wong, "Hackers Linked to China's Army Seen From EU to D.C."
124. Ibid.
125. Ibid.
126. Christopher Bodeen, "Chinese Hackers Take Weekends Off," *The Huffington Post*, February 25, 2013, http://www.huffingtonpost.com/2013/02/25/chinese-hackers_n_2756914.html.
127. "China Says U.S. Hacking Accusations Lack Technical Proof," *Reuters*, February 20, 2013, http://www.reuters.com/article/2013/02/20/us-china-hacking-idUSBRE91I06120130220.
128. Bodeen, "Chinese Hackers Take Weekends Off."
129. Josh Halliday, "Stuxnet Worm Is the 'Work of a National Government Agency," *The Guardian*, September 24, 2010, sec. Technology, http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency.
130. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED*, November 3, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

131. Halliday, "Stuxnet Worm Is the 'Work of a National Government Agency."
132. Ellen Nakashima and Joby Warrick, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say," *The Washington Post*, June 1, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.
133. Ibid.
134. "Defensie Zoekt 150 'Cyber-Reservisten,'" *NU*, November 2, 2013, http://www.nu.nl/internet/3618029/defensie-zoekt-150-cyber-reservisten.html.
135. "Klaar voor digitale strijd," nieuwsbericht, *Defensie*, (May 1, 2015), https://www.defensie.nl/actueel/nieuws/2015/05/01/klaar-voor-digitale-strijd.
136. Brien Posey, "Hiring Hackers As Security Consultants," *WindowSecurity.com*, accessed September 15, 2015, http://www.windowsecurity.com/articles-tutorials/misc_network_security/Hackers-Security-Consultants.html.
137. Security penetration testing means that for a fee, hackers can attempt to hack into a company's network and then present the company with a report detailing the existing security holes and how those holes can be eliminated.
138. Posey, "Hiring Hackers As Security Consultants."
139. Gerry Smith, "Feds Turn To Hackers To Defend Nation in Cyberspace," *The Huffington Post*, August 8, 2011, http://www.huffingtonpost.com/2011/08/08/government-recruits-hackers-cyber-shortage_n_920795.html.
140. Ibid.
141. Security.nl, "UWV: Tekort Aan Hoogopgeleide Security-Specialisten," September 11, 2015, https://www.security.nl/posting/443041/UWV%3A+tekort+aan+hoogopgeleide+security-specialisten.
142. Adam Martin, "The FBI Is Losing the War on Cybercrime," *The Wire*, June 6, 2011, http://www.theatlanticwire.com/technology/2011/06/fbi-losing-war-cyber-crime/38550/.
143. "One in Four US Hackers 'Is an FBI Informer' | Technology | The Guardian," accessed September 14, 2015, http://www.theguardian.com/technology/2011/jun/06/us-hackers-fbi-informer.
144. Ed Pilkington, "LulzSec Hacker 'Sabu' Released after 'Extraordinary' FBI Cooperation," *The Guardian*, May 27, 2014, sec. Technology, http://www.theguardian.com/technology/2014/may/27/hacker-sabu-walks-free-sentenced-time-served.
145. "One in Four US Hackers 'Is an FBI Informer' | Technology | The Guardian."
146. Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (February 2011): 41–60, doi:10.1080/00396338.2011.555595.
147. Ibid.
148. "APT28: A Window Into Russia's Cyber Espionage Operations?" (Milpitas, CA: FireEye, October 2014), https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf.
149. Kathrin Hille, "Chinese Military Mobilises Cybermilitias," *Financial Times*, October 12, 2011, http://www.ft.com/intl/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz3hklhyqAp.
150. Klimburg, "Mobilising Cyber Power."
151. Stephen Foley, "Facebook Hires Hacker Who Started Sony War," June 29, 2011, http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-hires-hacker-who-started-sony-war-2304075.html.
152. Osborne Charlie and Zero Day, "Google Recruits Top PS3 Hacker for Project Zero," *ZDNet*, July 2014, http://www.zdnet.com/article/google-recruits-top-ps3-hacker-for-project-zero/.
153. Andy Greenberg, "iPhone Super-Hacker Comex, Let Go From Apple, Goes To Work For Google," Forbes.com, *Forbes*, (April 2013), http://www.forbes.com/sites/andygreenberg/2013/04/24/iphone-super-hacker-comex-let-go-

from-apple-goes-to-work-for-google/.

154. Sara Yin, "7 Hackers Who Got Legit Jobs From Their Exploits," *PCMAG*, June 2011, http://www.pcmag.com/slideshow/story/266255/7-hackers-who-got-legit-jobs-from-their-exploits.
155. Ibid.
156. Smith, "U.S. Government's Urgent Mission."
157. "U.S Defense Giants Are Hiring the Best Hackers They Can Find (with a Few Caveats) | VentureBeat | Security | by Richard Byrne Reilly," accessed September 14, 2015, http://venturebeat.com/2014/08/11/u-s-defense-giants-are-hiring-the-best-hackers-they-can-find-with-a-few-caveats/.
158. Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations," 2012, https://www.academia.edu/1261902/Leveraging_Cyber_Militias_as_a_Force_Multiplier_in_Cyber_Operations.
159. Based on Applegate's theory; see Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations"; Mikheil Basilaia, "Volunteers and Cyber Security – Options for Georgia" (Tallinn University of Technology, 2012), http://csbd.gov.ge/doc/Volunteers%20and%20Cyber%20Security%20-%20Options%20for%20Georgia.%20Mikheil%20Basilaia.pdf; Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, Inc., 2010).
160. Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations."
161. Basilaia, "Volunteers and Cyber Security – Options for Georgia."
162. Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations."
163. Rain Ottis, "Theoretical Offensive Cyber Militia Models," in *Leading Issues in Information Warfare and Security Research*, by Julie J. C. H. Ryan (Reading: Academic Publishing International Ltd., 2011), 131–44.
164. Carr, *Inside Cyber Warfare*.
165. Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations."
166. *BlackEnergy & Quedagh: The Convergence of Crimeware and APT Attacks* (F-Secure, 2014), https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.
167. Jim Finkle, "Russian Hackers Target NATO, Ukraine and Others: iSight," *Reuters*, October 14, 2014, http://www.reuters.com/article/2014/10/14/us-russia-hackers-idUSKCN0I308F20141014.
168. Pavel Polityuk and Jim Finkle, "Ukraine Says Communications Hit, MPs Phones Blocked," *Reuters*, March 4, 2014, http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.
169. Tim Maurer and Scott Janz, "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context," *International Relations And Security Network*, October 17, 2014, http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345.
170. "Crimea – The Russian Cyber Strategy to Hit Ukraine," *InfoSec Institute*, March 11, 2014, http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.
171. "Hackers Join In the Struggle for Crimea," *The Interpreter*, March 7, 2014, http://www.interpretermag.com/hackers-join-in-the-struggle-for-crimea/.
172. "The United States Cyber Challenge – The United States Cyber Challenge 1.1 (updated 5-8-09)," accessed August 3, 2015, https://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20(updated%205-8-09).pdf.
173. Ibid.
174. Hille, "Chinese Military Mobilises Cybermilitias."
175. Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations."

176. Basilaia, "Volunteers and Cyber Security – Options for Georgia."
177. Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations."
178. Ottis, "Theoretical Offensive Cyber Militia Models."
179. Carr, *Inside Cyber Warfare*.
180. Ory Okolloh, "Ushahidi, Or'testimony': Web 2.0 Tools for Crowdsourcing Crisis Information," *Participatory Learning and Action* 59, no. 1 (2009): 65–70.
181. D Ndirangu Wachanga, "Participatory Culture in an Emerging Information Ecosystem: Lessons from Ushahidi," *Communicatio* 38, no. 2 (August 2012): 195–212, doi:10.1080/02500167.2012.717348.
182. Robert Munro, "Crowdsourced Translation for Emergency Response in Haiti: The Global Collaboration of Local Knowledge," in *AMTA Workshop on Collaborative Crowdsourcing for Translation*, 2010, 1–4, http://jan.stanford.edu/pubs/munro2010translation.pdf.
183. Simcha Levental, "A New Geospatial Services Framework: How Disaster Preparedness Efforts Should Integrate Neogeography," *Journal of Map & Geography Libraries* 8, no. 2 (May 2012): 134–62, doi:10.1080/15420353.2012.670084.
184. Devon Curtis, *Politics and Humanitarian Aid: Debates, Dilemmas and Dissension* (London: Humanitarian Policy Group / Overseas Development Institute, 2001).
185. See, for instance, Anand Giridharadas, "Ushahidi – Africa's Gift to Silicon Valley: How to Track a Crisis," *The New York Times*, March 13, 2010, sec. Week in Review, http://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html. Patrick Meier, "Ushahidi & The Unprecedented Role of SMS in Disaster Response – Ushahidi," *Ushahidi*, February 23, 2010, http://www.ushahidi.com/blog/2010/02/23/ushahidi-the-unprecedented-role-of-sms-in-disaster-response. Joshua Goldstein and Juliana Rotich, "Digitally Networked Technology in Kenya's 2007–2008 Post-Election Crisis," Berkman Center Research Publication, Internet & Democracy Case Study Series, (2008), http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan042523.pdf. Levental, "A New Geospatial Services Framework."
186. Levental, "A New Geospatial Services Framework."
187. United Nations Foundation et al., *Disaster Relief 2.0 the Future of Information Sharing in Humanitarian Emergencies*. (Washington, D.C.; Berkshire, UK: UN Foundation & Vodafone Foundation Technology Partnership, 2011), http://www.globalproblems-globalsolutions-files.org/gpgs_files/pdf/2011/DisasterResponse.pdf.
188. Levental, "A New Geospatial Services Framework."
189. Ibid.
190. Nathan Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project" (Development Information Systems International, 2011), http://ggs684.pbworks.com/w/file/fetch/60819963/1282.pdf.
191. Jan Voordouw, "Question about Haiti Relief Effort and Cooperation," September 12, 2015.
192. Jose Vericat, "Open Source Mapping as Liberation Technology: An Interview with David Kobia," *Journal of International Affairs* 64, no. 1 (2010): 195.
193. Huiji Gao, Geoffrey Barbier, and Rebecca Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief," *IEEE Intelligent Systems* 26, no. 3 (2011): 10–14.
194. Ibid.
195. Dawn S. Booker, "Wiki Approaches to Wicked Problems: Considering African Traditions in Innovative Collaborative Approaches," *Development in Practice* 24, no. 5–6 (August 18, 2014): 672–85, doi:10.1080/09614524.2014.934786.

196. Christopher Connell, "In Haiti's Hour of Need, Texting '4636' Became a Lifeline," *IIP Digital*, February 19, 2010, http://iipdigital.usembassy.gov/st/english/article/2010/02/20100219131612berehellek5.066395e-06.html#axzz3kfrZVehY.
197. Diasporas have played a significant role in numerous humanitarian disaster responses, for instance after the Gujarat earthquake in India or the Indian Ocean Tsunami. To see a brief discussion on the current relationships between the diasporas and the relief community, see "Diaspora Engagement in Humanitarian Response Paper" (International Organization for Migration, May 2015), http://unobserver.iom.int/sites/default/files/FINAL%20Paper%20-%20Diaspora%20and%20Humanitarian%20Response%20-%20May%202015.pdf.
198. Patrick Meier, "Haiti: Where We Are & Where We Go From Here – Ushahidi," *Ushahidi*, January 30, 2010, http://www.ushahidi.com/blog/2010/01/30/haiti-where-we-are-where-we-go-from-here.
199. Gao, Barbier, and Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief."
200. Robert Munro, "Crowdsourcing and the Crisis-Affected Community: Lessons Learned and Looking Forward from Mission 4636," *Inf Retrieval Information Retrieval* 16, no. 2 (2013): 210–66.
201. Gao, Barbier, and Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief."
202. Ibid.
203. Munro, "Crowdsourcing and the Crisis-Affected Community."
204. "About MMOWGLI," *MMOWGLI Portal*, accessed October 7, 2015, https://portal.mmowgli.nps.edu/game-wiki/-/wiki/10773/About+MMOWGLI.
205. Voordouw, "Question about Haiti Relief Effort and Cooperation."
206. Meier, "Haiti: Where We Are & Where We Go From Here – Ushahidi."
207. Ibid.
208. Björn-Sören Gigler and Savita Bailur, *Closing the Feedback Loop: Can Technology Bridge the Accountability Gap?* (World Bank Publications, 2014), http://public.eblib.com/choice/publicfullrecord.aspx?p=1711528.
209. See, for instance, Wachanga, "Participatory Culture in an Emerging Information Ecosystem." and Jocelyne Bourgon, *A New Synthesis of Public Administration Serving in the 21st Century* (Montreal: McGill-Queen's University Press, 2011), http://site.ebrary.com/id/10577863.
210. H Unabor, "Geospatial Response with Remote Sensing, GIS, OpenStreetMap and Ushahidi: The Haiti Eartchquake of 12th Januarry, 2010," *International Journal of Scientific & Engineering Research* 5, no. 2 (February 2014), http://www.ijser.org/paper/Geospatial-Response-with-Remote-Sensing-GIS-OpenStreetMap.html.
211. Gao, Barbier, and Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief."
212. Voordouw, "Question about Haiti Relief Effort and Cooperation."
213. Jessica Heinzelman and Carol Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti" (Washington, DC: United States Institute of Peace, 2010), http://dspace.africaportal.org/jspui/bitstream/123456789/29753/1/Crowdsourcing%20Crisis%20Information%20in%20Disaster%20-%20Affected%20Haiti.pdf.
214. Ibid.
215. Munro, "Crowdsourced Translation for Emergency Response in Haiti."
216. Quoted in Heinzelman and Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti," 9.
217. Heinzelman and Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti."
218. "Open Street Map Community Responds to Haiti Crisis," *Open Knowledge Blog*, January 15, 2010, http://blog.okfn.org/2010/01/15/open-street-map-community-responds-to-haiti-crisis/.

219. "Student Initiatives," *The Fletcher School | Tufts University*, accessed September 15, 2015, http://fletcher.tufts.edu/Hitachi/Student-Initiatives.
220. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
221. Patrick Meier, "Haiti: Taking Stock of How We Are Doing – Ushahidi," *Ushahidi*, February 7, 2010, http://www.ushahidi.com/blog/2010/02/07/haiti-taking-stock-of-how-we-are-doing; Heinzelman and Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti."
222. See for instance Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project." Booker, "Wiki Approaches to Wicked Problems."
223. Gao, Barbier, and Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief."
224. F. A. Mora, "Innovating in the Midst of Crisis: A Case Study of Ushahidi," *Submitted for Publication to SAGE Convergence Journal*, 2011, http://www.researchgate.net/profile/Fernando_Mora3/publication/231537244_Innovating_in_the_midst_of_crisis_A_case_study_of_Ushahidi/links/0fcfd506b9fdd4086b000000.pdf.
225. Booker, "Wiki Approaches to Wicked Problems."
226. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
227. Vericat, "Open Source Mapping as Liberation Technology."
228. Okolloh, "Ushahidi, Or'testimony'."
229. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
230. Patrick Meier, "We Are The Volunteers of Mission 4636 – Ushahidi," *Ushahidi*, January 27, 2010, http://www.ushahidi.com/blog/2010/01/27/we-are-the-volunteers-of-mission-4636.
231. Shadrock Roberts and Karen Payne, "Operationalizing VGI for Humanitarian Response: Is It Possible and What Does It Mean," in *Association of American Geographers Conference on Volunteered Geographic Information*, 2011, http://vgi.spatial.ucsb.edu/sites/vgi.spatial.ucsb.edu/files/file/aag/Roberts_abstract.pdf.
232. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
233. Friederike Schultz, Sonja Utz, and Anja Göritz, "Is the Medium the Message? Perceptions of and Reactions to Crisis Communication via Twitter, Blogs and Traditional Media," *Public Relations Review Public Relations Review* 37, no. 1 (2011): 20–27.
234. Unabor, "Geospatial Response with Remote Sensing, GIS, OpenStreetMap and Ushahidi: The Haiti Eartchquake of 12th Januarry, 2010."
235. Gao, Barbier, and Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief."
236. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
237. Quoted in Ibid., 16.
238. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
239. Munro, "Crowdsourcing and the Crisis-Affected Community."
240. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
241. Munro, "Crowdsourcing and the Crisis-Affected Community."
242. Ibid.
243. Gao, Barbier, and Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief."
244. Heinzelman and Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti."
245. Francesco Mancini, ed., "New Technologies and Conflict Prevention in Sudan and South Sudan," in *New Technology and the Prevention of Violence and Conflict* (New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013), 71–86.

246. Francesco Mancini, ed., "Early Warning and the Role of New Technologies in Kenya," in *New Technology and the Prevention of Violence and Conflict* (New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013), 42–55.
247. Francesco Mancini, ed., "Using Information and Communication Technologies for Violence Prevention in Latin America," in *New Technology and the Prevention of Violence and Conflict* (New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013), 28–41.
248. Francesco Mancini, ed., "Big Data for Conflict Prevention: New Oil and Old Fires," in *New Technology and the Prevention of Violence and Conflict* (New York, NY: United Nations Development Programme; United States Agency for International Development; International Peace Institute, 2013), 4–27.
249. Ibid., 20.
250. Mora, "Innovating in the Midst of Crisis."
251. Morrow et al., "Independent Evaluation of the Ushahidi Haiti Project."
252. Heinzelman and Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti."
253. Vidya Spandana, "Bittersweet Farewell to SwiftRiver – Ushahidi," *Ushahidi*, December 8, 2014, http://www.ushahidi.com/blog/2014/12/08/bittersweet-farewell-swiftriver.
254. Sophie Shepard, "Designing the Front-End of Ushahidi V3 – Ushahidi," *Ushahidi*, February 25, 2015, http://www.ushahidi.com/blog/2015/02/25/designing-the-front-end-of-ushahidi-v3.
255. Daudi Were, "Ushahidi Version 3.0 Is Here – Ushahidi," *Ushahidi*, August 19, 2015, http://www.ushahidi.com/blog/2015/08/19/ushahidi-version-3-0-is-here.
256. Patrick Meier, "Introducing Ushahidi SWAT – Ushahidi," *Ushahidi*, August 1, 2011, http://www.ushahidi.com/blog/2011/08/01/introducing-ushahidi-swat/.
257. Galya B. Ruffer, "What Ushahidi Can Do to Track Displacement," *Forced Migration Review*, no. 38 (oktober 2011): 25–26.
258. Heinzelman and Waters, "Crowdsourcing Crisis Information in Disaster-Affected Haiti."
259. Ibid.
260. Ibid.
261. Shadrock Roberts, "Supporting Online Volunteer Response to the Nepal Earthquake – Ushahidi," *Ushahidi*, April 25, 2015, http://www.ushahidi.com/blog/2015/04/25/supporting-online-volunteer-response-to-the-nepal-earthquake.
262. Ibid.
263. Angela Oduor Lungati, "Connecting Digital Networks to Strengthen Electoral Processes: A NEW SIGN OF HOPE," *Ushahidi*, April 24, 2015, http://www.ushahidi.com/blog/2015/04/24/connecting-digital-networks-to-strengthen-electoral-processes-a-new-sign-of-hope.
264. Roberts, "Supporting Online Volunteer Response to the Nepal Earthquake – Ushahidi."
265. Ibid.
266. E. B. Boyd, "State Department Is Trying To Make A Thousand Ushahidis Bloom," *Fast Company*, accessed September 15, 2015, http://www.fastcompany.com/1751308/state-department-trying-make-thousand-ushahidis-bloom.
267. Ibid.
268. For a list of "deployments of the week" on the Ushahidi's wiki website, see Heather Leson, "Deployments of the Week," *Ushahidi Wiki*, 2015, https://wiki.ushahidi.com/display/WIKI/Deployments+of+the+Week.

269. Clingendael and HCSS, " Internationale Materieelsamenwerking. Rapport ten behoeve van het Interdepartementaal Beleidsonderzoek (IBO) naar internationale samenwerking op het gebied van defensiematerieel", Janury 2015, bijlage 3 and 4.
270. Stephan De Spiegeleire et al., "Commentary," in *Bridging the Collaboration Gap: Results from a Global Defense Survey on Collaboration During Coalition Operations* (Somers, NY: IBM, 2009), https://www.ibm.com/smarterplanet/global/files/us__en_us__government__gbe03231usen.pdf.
271. Many NGOs don't want to be (formally) associated with government agencies because it might put their impartiality – or the perception thereof – in jeopardy.
272. On this, see also Carlota Perez, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages* (Cheltenham UK; Northampton MA USA: Edward Elgar Publishing, 2002); Mansel G. Blackford, *The Rise of Modern Business: Great Britain, the United States, Germany, Japan, and China* (UNC Press Books, 2012); David S. Landes, Joel Mokyr, and William J. Baumol, eds., *The Invention of Enterprise: Entrepreneurship from Ancient Mesopotamia to Modern Times* (Princeton, N.J.: Princeton University Press, 2012).
273. Richard R. Nelson, *Technology, Institutions, and Economic Growth* (Harvard University Press, 2005), 197.
274. Blackford, *The Rise of Modern Business*.
275. The term was introduced by a 2002 report by the U.S. National Science Foundation and Department of Commerce. See Mihail C. Roco and William Sims Bainbridge, eds., *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science* (Dordrecht ; Boston, Mass: Kluwer Academic Publishers, 2003); Mihail C. Roco et al., *Convergence of Knowledge, Technology and Society: Beyond Convergence of Nano-Bio-Info-Cognitive Technologies* (Springer Science & Business Media, 2014).
276. On the crucial and growing importance of information, see James Gleick, *The Information: A History, a Theory, a* Flood (HarperCollins UK, 2011).
277. "China Takes Lead On The 2015 Global 2000," *Forbes*, accessed October 26, 2015, http://www.forbes.com/global2000/list/; "Fortune 500 – Fortune," 500, accessed October 26, 2015, http://fortune.com/fortune500/.
278. "the concept of loose coupling also holds tremendous promise in transforming how executives organize business processes, especially as they extend across global business enterprises" (Hagel, Brown, The Joy of Flex)"

The Hague Centre for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
HCSS.NL