The EU's Border and Coast Guard Agency, Frontex, was established in 2005 to “coordinate operational cooperation between Member States in the management of the EU’s external borders; assist Member States in circumstances requiring technical and operational assistance at external borders; and provide Member States with the necessary support in organizing joint return operations” (Reg. No. 2007/2004). The agency is also equipped to undertake risk analyses, research, training, and emergency response operations to facilitate the integration of border management by EU Member States.

Frontex’s conduct at EU’s external borders, however, has been heavily criticized by non-governmental organizations, EU Agencies, and international organizations. Its activities were responsible for and contributed to systematic pushbacks of migrants in the Canary Islands and in the Mediterranean Sea as well as on the Greek and Bulgarian border. These activities violated human rights because Frontex failed to identify asylum seekers and thus returned migrants to situations where they could face persecution on the grounds of the 1951 Refugee Convention. The pushback operations contributed to migrants taking even more dangerous routes across the sea and thus impacted the rise of deaths at sea. According to the Missing Migrants Project by the International Organization of Migration, there has been a steady increase in migrant deaths in the Mediterranean Sea since 2014.[1] What accounts for the human rights violations committed by Frontex? During the same period, the technological apparatus behind EU border management also increased in sophistication. For example, Frontex’s European Border Surveillance System (EUROSUR) started to operate by the end of 2013. It is a Europe-wide system equipped with satellite surveillance, real time situational pictures, and operational forces on the ground that keep a close eye on migration movements. If one compares the recent increase in the numbers of deaths at sea to the developments in technological surveillance, one wonders what kind of norms and conceptual approaches are attached to the introduction of new technology in EU border management. This paper tries to put human rights violations in the context of the recent developments in the border management system of the EU.

The literature on human rights violations committed by Frontex is manifold. While some argue that the preeminence of security concerns shape the practices of border management activities, others point toward institutional features that enable Frontex to operate in legal grey zones. Others assert that the asylum and migration policies of Member States influence the way Frontex operates on the ground. This paper suggests that a larger phenomenon might be at play. It argues that human rights violations committed by Frontex are an unanticipated consequence of the diffusion of military technology and ideas. It argues that there is evidence to suggest that military knowledge of network-centric operations has shaped EU border management. Although this paper cannot trace the precise steps of this diffusion for parsimonious reasons, there are, however, compelling similarities in military and border management thinking that could inspire the continuation of research of this issue.

The next section will review the main literature on human rights violations by Frontex. Afterwards, Diffusion of Innovation Theory (DOI) will be introduced and put into the context of military technologies and ideas. The case study that follows will compare the similarities between EU border management and the concepts of network-centric warfare. The paper will end with a discussion of the findings and suggestions for future research.

**Literature Review: Factors that explain human rights violations by Frontex**

Frontex has been criticized by EU agencies, non-governmental organizations and international organizations for...
failing to uphold the right to life, the respect for human dignity, the right to asylum, and the right not to be subjected to torture or inhumane or degrading treatment. The literature that provides explanations for these violations can be divided into three schools of thought: ideas; institutional perspectives; and interest-based approaches.[2]

Ideas as a Source of Human Rights Violations

The common theme across this literature is the persistence of security as a fundamental value in border management. Other concerns, such as humanitarian relief, human rights protection, saving lives at sea, or creating legal avenues for migration remain a secondary priority. These authors argue that a security-oriented approach is reflected in the nature of Frontex (Statewatch, 2013; Perkowski, 2012; Perkowski, 2012a; Léonard, 2010; Frontexit, 2014; European Parliament, 2015; Carling & Hernández-Carretero), in the development of Frontex supporting institutions (Rijpma & Vermeulen, 2015; Heller & Jones, 2014), in the allocation of funds (Amnesty International; 2014; HRW, 2014; HRW, 2015), in the working arrangements with third countries (Keller et al, 2011, HRW, 2016a), and in the training and mindset of border guards (Statewatch 2017; Franko-Aas & Gundhus, 2015).

It is argued that the origins of Frontex lay in the association of migration with terrorism and organized crime (Perkowski, 2012a), whereby ‘irregular migration’ became a security concern (Statewatch, 2013). The logic behind Frontex is, thus, the surveillance and protection of EU’s external borders with a focus on preventing risks, identifying threats, and combatting irregular migration and cross-border crime (Frontexit, 2014: 3; European Parliament, 2015: 39). EUROSUR’s founding regulation, for example, stresses that it can, “at most,” contribute to ensuring protection and saving lives at sea (Rijpma & Vermeulen, 2015: 467; Heller & Jones, 2014). Compliance with human rights is also not a precondition for working arrangements between Frontex and third countries (Keller et al, 2011: 29, HRW, 2016a). Finally, there is also an emphasis on border guards in the literature. Some point out that guidelines for border patrol agents do not mention anything about duties of care and protection (Statewatch, 2017). In another article, border agents are being described as maintaining a policing mindset. This mindset makes them view migrants as a source of information about crime activities and not as subjects in need of international protection (Franko-Aas & Gundhus, 2015: 6-9).

Institutional Perspectives on Human Rights Violations

The vast amount of literature that critically analyzes Frontex from an institutional perspective focuses on accountability, transparency, legal ambiguities, and specific facets of its operations.[3] To summarize, they identify unclear political and legal clarity over how and who is managing the EU’s external borders as a key issue. This enabled Frontex to make and interpret border control practices, extend the territorial limits of the EU’s external borders, and conclude bilateral agreements with third countries without the involvement of Member States. The results were unlawful control practices; opening new control fronts across the Mediterranean Sea; and the externalization of border management to third countries whose human rights records are problematic (Reid-Henry, 2013: 209-16).

Furthermore, Frontex enjoys little democratic oversight and regulation by the European Parliament (EP), the Court of Justice, and the public. Neither can they regulate its working programs, risk analyses, evaluations, operational agreements, and joint operations with third countries, nor do they have they access to them. Without oversight, there is little debate over the legality of missions. Frontex’s competencies are also not clearly defined and oftentimes get blurred with the competencies of Member States. There is no clear mechanism that allocates the legal responsibilities of border agents during missions. Additionally, Frontex is not required to provide details on how it identified asylum seekers or how it ensured that nobody was subjected to refoulement. Without knowledge of the controls carried out, it becomes difficult to assess Frontex’s compliance with human rights or hold Frontex staff accountable for human rights violations.

Moreover, there is no obligation to search and rescue ships on high seas; a loophole often instrumentalized to avoid responsibilities to launch rescue missions (Heller & Jones, 2014). Franko-Aas and Gundhus argue that
Frontex’s inaction to help migrants in distress may be related to the fact that it does not include migrant mortality rates in its performance evaluations: “Knowledge of death is therefore intrinsically connected to an acknowledgement of death; it is a denial of invisibility of dead bodies. To be countable therefore presupposes that one is recognized as countable” (2015: 11-12). Its performance measures only assess the vulnerabilities of EU external borders and suggest ways how to minimize them.

Interest-based Approaches to Human Rights Violations

The literature on interest-based approaches asserts that Frontex’s functions are affected and rooted in the “highly restrictionist and exclusionary immigration policy framework” of Member States (Perkowski, 2012a; Langford, 2013: 250). Member States pushed for tighter controls of EU borders by increasing patrols at sea, more cooperation with countries of origin and transit, and more efficient coordination of return operations (Giannetto, 2014). The reason behind the externalization of border management is due to ‘venue shopping’ by Member States for the benefit of their law enforcement agents. One outcome of that was joining police actors to cooperation networks with Frontex as a central coordinator. This in turn lifts the responsibility of control operations from Member States (Marin, 2011: 487). Sometimes, however, disagreement over new regulations on issues, such as search and rescue; broadening the definition of distress; interception; or establishing binding rules about where rescued migrants should be taken to, may lead to stagnation or even non-cooperation by Member States (Rijpma & Vermeulen, 2015: 467; HRW, 2013). Malta, for example, opted out of directing joint operations, because it argued that this would disproportionately affect its domestic migration system. Member States can also be forceful in pursuing their own interests, despite credible objections by democratic actors in the EU. For example, in the drafting of the regulation establishing Frontex, the EP suggested to include provisions for human rights, and to assess the need of a European Border Guard and its added value. Additionally, the EP petitioned to be able to review Agency evaluations. Member States, however, ignored these concerns in the final text of Regulation 2007/2004 (Léonard, 2009: 384).

Each explanation provides valuable insight into understanding systematic human rights violations by Frontex. On their own, however, they do not explain the origins and mechanisms that underlie the perpetuation of human rights violations. Perhaps these explanations are symptomatic of a much larger phenomenon. This paper argues that human rights violations are a result of the unanticipated consequences of the diffusion of military technology and ideas into the EU border management apparatus. DOI might offer a helpful explanation and act as a theoretical and empirical bridge between these different approaches to human rights violations by Frontex.

Theory & Methodology: The Diffusion of Military Technology and Ideas

The most commonly known definition of diffusion is provided by Rogers, who explained that it is “a process in which an innovation is communicated through certain channels over time among members of a social system” (2003: 5). Within the context of military technology and ideas, diffusion is defined by “how military knowledge […] diffuses throughout the international system, or what factors enhance or inhibit the ability of states to incorporate innovations into their defense structures” (Goldman & Eliason, 2003a: 7). What is being diffused is referred to as ‘hardware’ and ‘software.’ While hardware describes the physical tools that embody an innovation, software denotes the organizational and human application—the doctrines of an innovation (Rogers, 2003:13; Goldman & Eliason, 2003a: 8). The two principal actors in the diffusion process are the change agent and the adopter. The former influences the innovation-decision of the latter (Rogers, 2003: 27). Researchers use process tracing to trace the causal pathways—causes, transmission paths, and consequences—for diffusion of innovations (Goldman & Eliason, 2003a: 22).

The causes that drive the spread of new military innovations emanate from major structural forces; strategic necessity; economic pressure; technology-push dynamic; and institutional pressure. It is possible that competition in the international system can induce states to adopt military innovations from powerful actors. The industrial-military complex, which has strong institutional and financial interests in the spread of new military technology, can also exert powerful economic pressure that enables diffusion. The dual-use application of new technology in the commercial and military sectors may also encourage diffusion processes. Lastly, institutional pressures could...
Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel

incentivize the adoption of military innovations if they enhance the resources, autonomy, and the essence of an organization (Goldman & Eliason, 2003: 374).

Multiple transmission paths for the spread of innovations exist. According to diffusion literature, there are competitive, voluntary, and collaborative processes. *Emulation*, or ‘policy bandwagoning,’ describes how elites watch successful policy changes abroad in order to copy similar policies domestically. This kind of diffusion is most likely to succeed when the change agent and the adopter share similar cultural and social settings. *Elite networking*—via policy communities, issue networks, epistemic communities, or transnational networks—facilitate diffusion through the interaction and consensus-making among elites. Through the use of professional organizations, meetings, and journals, experts and practitioners develop common approaches and create established knowledge about how to solve certain problems and how to define the problems that are to be solved. The introduction of new technologies into these communities can lead to the redefinition of problems and to changes in the ways they are approached. *Harmonization* is a process where a group of transnational actors coordinate their policies based on consensual knowledge embedded in intergovernmental and supranational institutions. In this model, mutual recognition of the interdependence between the actors—“reliance on others for the performance of specific tasks to ensure complete and successful implementation”—drives policy convergence (Goldman & Eliason, 2003a: 15-17).

Successful diffusion eventually leads to alterations in the structure and functions of a *social system*. Diffusion is, however, less deterministic than the previous statement makes it seem. New technologies don’t exist in a cultural and organizational vacuum. Culture and local institutions influence the ways in which military organizations integrate innovations into their operations. The rate of adoption is dependent on several factors and the adopter also modifies some innovations during adoption and implementation (Goldman & Eliason, 2003a: XV, 9; Rogers, 2003: 17).

It is thus paramount to understand the systematic consequences of diffusion. Rogers classifies the consequences as *desirable* vs. *undesirable*, *direct* vs. *indirect*, and *anticipated* vs. *unanticipated*. The distinction between desirable and undesirable consequences indicates functional and dysfunctional effects of an innovation for a social system. For example, undesirable consequences can negatively affect a social system’s qualities. While direct consequences affect a social system in the immediate response to the adoption of an innovation, indirect consequences come about as the result of direction consequences of the adoption of an innovation. Finally, the changes to a social system that are recognized and intended by its members are anticipated consequences. Those changes that are neither intended nor recognized by the members of a social system are unanticipated consequences. Unanticipated consequences are indicative of a lack of understanding by the change agent about the functions of an innovation and the forces at play in a social system (Rogers, 2003: 442-49).

The insight into the causes, transmission paths, and consequences for diffusion, which were discussed above, will serve as a theoretical guide for the next section. The section that follows will highlight critical connections between the U.S. Military’s *network-centric warfare* (NCW) and the European Union’s Integrated Border Management (IBM). The argument is that the Information Age, which functioned as a structural force, created incentives for the commercial sector to develop network-centric operations in the 1970s. The U.S. Military sector adopted hardware and software associated with this innovation in the 1990s and integrated them into its military operations. This article suggests that the hardware and software associated with the U.S. Military’s reinvention of network-centric operations diffused into EU border management Although this paper cannot trace the precise steps of the diffusion of NCW to EU border management for parsimonious reasons, there are, nevertheless, compelling similarities in their hardware and software that could inspire the continuation of research on this issue.

**Case Study: EU Border Management and the Diffusion of Military Innovations**

In the 1980s, Toffler & Toffler wrote that our world economy moved from the Industrial Age into a new century. While the Industrial Age economy was based on raw materials and physical labor, a new, revolutionary economy arose based on *knowledge*: the Information Age (1993: 3). In a nutshell, the Information Age altered wealth-production and the distribution of power; increased complexities; shrunk distances around the world; and
increased the speed of our lives (Alberts et al, 2000: 15). While military organizations were in the vanguard of
developing new technologies in the past, the demands by the commercial sectors drove major IT advances in the
Information Age. The increased utilization of new IT led to the coevolution of new innovations that enhanced value
production for customers. By shifting to network centric enterprise, the most dominant competitors acquired
information superiority and used it to their advantage (Alberts et al, 2000: 1-2).

These unparalleled changes to our world economy also brought about innovations in the nature of warfare. If it is
true what Toffler & Toffler argue, that “the way we make war reflects the way we make wealth,” it is equally
interesting to ask, whether the way we protect our borders might reflect the way we make war (1993: 2-3). There
is evidence to suggest that the changes to the nature of warfare, which were generated by advances in IT, show
similarities to recent developments in the EU’s border management apparatus. This case study will explain these
similarities in the context of the Information Age’s innovative changes to military operations.

The Information Age, the commercial Sector, and network-centric Enterprise

Writing for U.S. Department of Defense (DoD), Alberts et al. outline the Information Age’s impact on the
commercial sector. The reason why commercial organizations were compelled to adopt Information Age concepts
and technologies lay in the changes to the laws of competition. These new concepts and technologies led to a
drop in the costs of production and distribution, and the lowering of barriers to enter new markets, indirectly
undermining the competitive advantage of prominent organizations. In order to hold competitive advantage[8] in
the market—that is information superiority[9]—organizations needed to come up with more effective ways of value-

In this period, the creation of value was closely associated with networks. Organizations followed Metcalfe’s law,
arguing that “as the number of nodes in a network increases, the potential ‘value’ or ‘effectiveness’ of the
network increases exponentially as the square number of nodes in the network” (Alberts et al., 2000: 32). The aim
was to pursue information-based strategies by linking the activities[10] in the value chain and becoming a network-
centric enterprise (NCE). This generated a whole series of concurrent activities needed to survive in the market. A
high level of awareness of developments[11] in the business environment was crucial to initiating strategies to
enhance one’s operational effectiveness. The better the situational awareness, the more successful risk analyses
were conducted.[12] Companies needed to work as a virtual organization[13] to improve the product design
process, facilitate concurrent processing, and boost responsiveness to changes in customer needs. For example,
enterprises like Capital One, Dell, or Wal-Mart run successful information-based strategies that lifted their

Capital One developed sophisticated analytical techniques on default rates to manage operational risks of its
lending practices. Dell’s ‘sense and respond’ model[14] allowed rapid response to the demands of customers,
with up-to-date information on the state of its products. The constant real time sharing of information enabled Dell
to develop a common operational picture, thus improving the speed, flexibility, and responsiveness of production.
Finally, Wal-Mart developed sensory capabilities through sales scanners that collected information on all
transactions. It shared this information with its suppliers in near real time and was able to effectively control

From network-centric Enterprise to network-centric Warfare

Concomitant with the developments in the commercial sector were the changes in the nature of warfare. Alberts
et al. writes, “[w]e see the lessons learned in the commercial sector not as gospel to be blindly followed, but as
inputs to our concepts, development, and experimentation processes.” (2000: 26). The primacy of information as
a source of power is equally important in network-centric warfare (NCW). In a nutshell, NCW is an “information
superiority-enabled concept of operations that generates increased combat power by networking sensors,
decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo
operations […] and a degree of self-synchronization” (Alberts et al., 2000: 2). It has reinvented the command and
control structures in military operation via the networked usage of information technologies. Developments in IT
were critical to the increase in computing power and transmission capabilities; surveillance and sensor capabilities (to spot, identify, and track targets); and the ability to hit target more precisely and quickly (Osinga, 2010: 22-23).

The basic premise is the development of an information structure that facilitates shared battlespace awareness and knowledge for the people involved to influence the outcome through the adaption of C2 approaches. The Information Age allows geographically dispersed forces to be more informed and effective while ‘on the move.’ This, in turn, comes from a shared awareness of the combat environment as well as a shared knowledge of operational intent. An accurate and robust information structure leads to a force that is able to self-synchronize, increase the tempo of operations and responsiveness, lower risks and costs, thus increasing combat effectiveness (Alberts et al., 88-93).

Similarities between network-centric Warfare and the EU Border Management System

Although one cannot definitively demonstrate the diffusion of network-centric warfare into EU border management within the range of this paper, this section will show some similarities between the concepts and approaches of NCW and the EU’s border management system. There is evidence to suggest that the commercial sector could have been the change agent of diffusion as well. Nonetheless, it is interesting to note that the introduction of NCW to the U.S. Armed Forces (2001-2006) almost coincided with early conceptual developments in EU migration management (1999-2004). It is interesting because the U.S. Military was in frequent contact with EU Member State’s militaries via NATO during this period. NATO may be one venue where diffusion could have taken place.

This section will analyze the EU border management concepts a) Integrated Border Management; b) Risks Analyses; and c) Rapid Border Intervention Teams (RABIT) in the context of NCW. While the first one will provide a conceptual and practical overview of the how the EU envisioned and has implemented its border management system, the latter two are specific approaches to its border management that are identical to the ‘Sense and Respond’ model discussed earlier.

a) Integrated Border Management

Frontex is the central actor responsible[15] for the implementation of the integrated border management (IBM) concept of the EU—a network-centric, near real time operating information exchange between Member States (Wagner, 2009: 19). Since the 1999 Tampere Program, IBM has been central to the EU’s border management. The notion behind IBM is to link Member States’ border control and surveillance activities (Léonard, 2010: 234). The EU developed a four-tier access control model to put Frontex’s activities into a network of concurrent processes. The EC explains that this model combines “control mechanisms and tools, based on flows of persons into the EU. It involves taking measures at the consulates of the Member States in non-EU countries; measures in cooperation with neighboring non-EU member countries; measures at the border itself; and measures within the Schengen area” (Hayes et al., 2014: 67).[16]

Additionally, the European Border Surveillance System (EUROSUR) has been crucial to Frontex’s ongoing border management since 2013. EUROSUR coordinates and develops the intelligence-driven operational cooperation (Neal 2009: 333). That means synchronizing Member States’ existing surveillance systems,[17] developing and implementing EU-wide surveillance technology,[18] and establishing a shared information environment of domains around the EU. The appropriate network for the fulfillments of these tasks consist of a centrally operating headquarter, joint National Coordination Centers (NCCs), and working arrangements with third countries (Marin, 2011: 140-42). With the information provided through this network, Frontex forms National Situational Pictures, the European Situational Picture, and the Common Pre-Frontier Situational Picture—real time situational awareness of the migration movements within, close to, and far outside the EU (Marin, 2014: 11).[19] The IBM operates, thus, very similarly to the NCW’s strategy for information superiority via shared battlespace awareness.

b) Common Integrated Risk Analysis Model
Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel

Former director of Frontex, Ilka Laitinen, emphasized early on that “[a]ll FRONTEX activities are based on risk analyses, the ‘engine’ of FRONTEX activities” (2006). The modus operandi is based on the Common Integrated Risk Analysis Model that embodies a very technocratic concept of ‘risk.’ The risk assessment functions are cognizant of the so-called ‘threat’ of migratory flows and the capacities of EU Member States to manage their borders (Neal, 2009: 346-47). A key performance measure is the analysis of ‘vulnerabilities.’ This term refers to the vulnerabilities of borders and includes facets, such as its geographical characteristics, the effectiveness of border control, existing return agreements, and the presence of diasporic communities—that could be migratory pull factors. Any migrant—irregular, economic, asylum seeking, etc.—is defined via this model’s risk measures, thus, as a threat by default.[20] The model defines ‘threat’ as a ‘force or pressure acting on the external border.’ The various indicators included in this category are factor including but not limited to numbers of refused entries, third country nationals apprehended or facilitators intercepted (Franko-Aas & Gundhus, 2015: 9-10).

It comes as no surprise that many—and even the Agency itself—describe Frontex as an “intelligence-driven organization” (Léonard, 2010: 243); a concept usually applied to information gathering operations related to threats to national security. A compelling similarity between Frontex and military organizations is thus the organizational edifice producing and disseminating information on the migration flows towards the EU. Frontex’s Situational Centre (FSC) is of particular focus in that regard. Its aim is to develop a real time picture of the migration situation at EU’s external borders. It also has the capacity to issue emergency response mechanisms in critical moments. These functions are reminiscent of NATO’s Situation Center (SITCEN), the UN’s Peacekeeping Situation Center, and the EU’s Joint Situation Centers that all focus on traditional security threats, such as terrorism or the proliferation of WMDs (Léonard, 2010: 243). The so called ‘engine’ of Frontex is thus indicative of a similarity between the NCW’s pursuit of shared battlespace awareness to lower risk factors and enhance combat effectiveness.

c) Rapid Border Intervention Teams

Aside from the ‘sense’ function of Frontex, the EU institutionalized a ‘respond’ function, represented by the Rapid Border Intervention Teams (RABIT) in 2007. It is a tool for Member States to be called upon to help when faced with urgent and exceptional migratory pressures (Frontex, 2017a)—such as “mass influx of third country nationals illegally attempting to enter a Member State’s territory (Marin, 2011: 136). When the aforementioned risk and intelligence activities are unsuccessful in predicting these events (see also footnote 20), Frontex deploys the European Border Guard Teams—that are part of RABIT.[21] From November 2010 to March 2011, Frontex launched its first RABIT operation at the Greek-Turkish Border, involving 200 border officers from 26 Member States (European Commission, 2011). Two things are noteworthy about RABIT: the powers of members of the team and the deployment structure of RABIT.

First, according to Article 6 of the RABIT regulation (EC/863/2007), the members deployed have the authority to reinstate border checks and border surveillance as indicated by the operational plan. The more interesting aspect of that, however, is that members of RABIT are authorized to carry and use service weapons in accordance with the law of the host state—usually for legitimate self-defense or for the defense of members of the team or other persons (Marin, 2011: 136-137). It is interesting because arming rapid response border guards may mimic operations of rapid response military forces. Second, RABITs are organized based on the principle of ‘compulsory solidarity.’ That means Member States must provide border guards to a so-called ‘Rapid Pool,’ a selected group that Member States are obligated to deploy at the request of Frontex (Léonard, 2010: 245)

In the context of diffusion of military technologies, RABIT is reminiscent of operational measures that have traditionally been created to deal with threats, such as a foreign-armed invasion or attack. This type of emergency response operation is now being used for migration. Furthermore, the notion that a group of states is obligated to mutual emergency response, in the name of solidarity, is very similar to NATO’s ‘solidarity clause’ (Léonard, 2010: 245). In general, RABITs share the conceptual thinking of NATO’s Response Force (NRF). The NRF is a multi-national force—created in 2002—with the capacity to provide a “rapid military response to an emerging crisis, whether for collective defense purposes or other crisis-response operations (NATO, 2017). Although the essence of operations differs, RABITs and NRFs are conceptualized similarly in their versatility (see footnote
There are a variety of explanations about the global diffusion of information technology for military purposes. While some assert that the reason for adoption lies in the fact that states view IT modernization as legitimate and modern (Demchack, 2003: 307-08), others look at market-based explanations that emphasize ‘industrial competitiveness’ (Hayes, 2010). Although this paper will not review the literature on the so-called ‘global spread of the information warfare,’ the case of the EU suggests possible transmission paths that could be assessed for their validity in future research.

In the area of Research & Development (R&D), Frontex has been cooperating with the defense and military industry within the context of the EU’s 7th Framework Program to incorporate military surveillance technologies. At least since 2002, big players of the war industry—Sagem, Finmeccanica, Israel Aircraft Industries and others, who are commonly known as the European Organization for Security (EOS)—are deeply involved in EU-sponsored research that develops technology with the purpose of achieving “24/7 blue and green border situation awareness” (Marin, 2011: 143-44; Hayes et al., 2014: 11). In the R&D cooperation, Frontex participated in workshops and seminars organized by the Commission, where it had frequent contact with actors as such the European Defense Agency (EDA), NATO, and the military industry. Through this participation, Frontex is kept up-to-date with so-called ‘civil-military synergies’ (Hayes et al., 2014: 65). Through lobbying, the arms and security industry exerts critical influence over European security policy. Its regular interaction with the EU not only shapes research; the lobby group is also successful in proposing policy changes to the EU’s security structure. The most recent change was the transformation of Frontex into the European Border and Coastguard Agency. Other venues of interaction are security fairs, such as the World Border Security Congress or the annual European Day for Border Guards (ED4BG). One observer of these events noted that at “these events, it is possible to identify a cyclical culture whereby the presentation of new technologies not only responds to, but also enables and drives the formulation of new policies and practices in the field of border security and migration management” (Akkerman, 2016: 23; Akkerman, 2016a: 15; MA., 2012; MA., 2013). There is, thus, critical evidence to suggest that elite networking plays a crucial role in the diffusion of military technology into the EU’s border management. Further research should trace the steps of these interactions because, most of the time, whatever happens in these meetings is not disclosed to the public.

Conclusion: Human Rights Violations as unanticipated Consequence of Diffusion (and the EU as a Change Agent?)

The campaign video by Frontexit ends with the phrase ‘Europe is at war against an imaginary enemy.’ To a certain degree, this phrase captures the essence of this paper. The involuntary involvement of migrants in this war subjects them to human rights violations caused by a border management that treats them as a statistical indicator and not as subjects that are eligible and in need of international protection. Where does this ‘war’ come from? There is compelling evidence suggesting that the diffusion of military technologies and ideas perpetuate a militarized approach to border management. While its intention is to reduce the number of ‘irregular’ migrants entering the EU via land and sea borders, its conceptual and practical approach, however, ignores its contribution to the continuation of violations against right to life, the respect for human dignity, the right to asylum, and the right not to be subjected to torture or inhumane or degrading treatment.

The EU’s border management (IBM, risk analyses, RABIT) share conceptual similarities with network-centric warfare. At the core of this similarity is the creation of an information structure that enhances one’s battlespace/ situational awareness of the targets/ migratory movements on the ground. This (near) real time awareness was provided by thorough sensing or risk analyses of the situation on the ground. In both, the military and EU migration context, sensing is done through sophisticated technological measures, such as satellites, drones, or on the ground forces. It is the combined effort of a network of various units that enable shared situational awareness. Finally, the military as well the EU is able to deploy rapid response units in cases of urgent and unexpected situations. The EU’s RABIT and NATO’s Response Force appear similar in their versatility and deployment.
Besides these similarities, EU appears to spread its border management approach to its immediate neighbors. Is Frontex becoming a change agent for the military technologies and ideas it has adopted? By 2010, Frontex operationalized the Africa-Frontex Intelligence Community—a working arrangement that develops intelligence operations based on its own risk analysis model (Grieger & Schlindwein, 2016). It has already finalized agreements with various countries but neither democratic institutions nor NGOs can exactly monitor what Frontex is doing in these countries with regard to migration. In other cases, it is clearer. As part of the readmission agreement with Turkey, Frontex states explicitly that Turkey must demonstrate that it “carries out adequate border checks and border surveillance along all the borders of the country, especially along the border with EU member states, in such a manner that it will cause a significant and sustained reduction of the numbers of persons managing to illegally cross the Turkish borders” (Amnesty International, 2014: 13). Amnesty International also reported that the EU has funded a project in the Southern Mediterranean to help Algeria, Egypt, Libya, and Tunisia to install a surveillance network that is able to inform the EU about “illegal or suspect activities” (2014: 28).

To conclude, future research should assess the impact of the interactions between Frontex and the military industry on human rights as well the impact of Frontex activities in third countries. This paper demonstrated that there is compelling evidence suggesting a link between the diffusion of military technology and ideas into the EU’s border management system. It has also provided insight into the possible transmission paths of this diffusion. More conclusive research on this topic can support human rights advocates and parliaments with ample evidence linking migrant’s human rights violations to EU’s security regime. This in turn will reinforce political and judiciary activities that seek to hold the actors—who are the most vocal and who profit the most from this ‘war against an imaginary enemy’—accountable.

Bibliography


Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel


Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel


Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel


Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel


PRO ASYL. (2013). “Pushed Back: systematic human rights violations against refugees in the Aegean sea and at the Greek-Turkish land border.” November, 7. PRO ASYL Foundation and Friends of PRO ASYL.


[1] In 2014, 3,274 were recorded dead (globally 5,265). In 2015, 3,784 were recorded dead in the Mediterranean Sea (globally 6,117). In 2016, a total of 5,098 people were recorded dead in the Mediterranean Sea (out of 7,565 recorded dead globally). As of March 13, 2017, 525 people were already recorded dead in the Mediterranean Sea (IOM, 2017).

[2] Baglione defines them as: “Interest-based approaches assert that actors make decisions that maximize their priorities […] these are often called rational-choice approaches. From this perspective, agents take steps that best serve their interests […]. Institutional perspectives focus on rules or structures of institutions and show that these established routines or patterns have an impact on outcomes. […] The third I here –ideas– is actually a catchall term for ideas, identities, and cultures. These type of explanations contend that what actors think, who they are (or who they think they are), and what they value determine results.” (2012: 48)


Linking the Diffusion of Military Ideas to Human Rights Violations at EU Borders
Written by Marcel Gretzschel

[5] Rogers defines a social system as “a set of interrelated units that are engaged in joint problem solving to accomplish a common goal. A system has structure, defined as the patterned arrangements of the units in a system, which gives stability and regularity to individual behavior in a system” (2003: 24, 37).

[6] Goldman & Eliason explain that the compatibility of an innovation with the existing values, practices, past experiences, and current need of adoption by the adopter influence the rate of adoption (2003a: 8).

[7] Rogers defines a social system’s qualities as including family bonds, respect for human life and property, maintenance of individual dignity and respect, and appreciation of others. To that end, he says: “An innovation may be functional for a system but not functional for certain individuals in the system” Rogers emphasizes the antagonism between effectiveness-convenience-efficiency and social values and institutions (2003: 443).

[8] Increase the relative value of products and services vis-à-vis competitors (Alberts et al., 2000: 31)

[9] Alberts et al. Describe information superiority as a condition where an organization hold competitive advantage due to fact that it enjoys a superior information position contra its competitors. It is the ability to “collect, process, and disseminate and uninterrupted flow of information while exploiting and/ or denying an adversaries ability to do the same” (2000: 34, 54).

[10] operations and production, marketing, sales and services, logistics, supporting activities, technological development, human resources, management, and general infrastructure (Alberts et al., 2000: 30)


[12] Risk analyses were conducted in order to suppress time and the cost of processing.

[13] Rogers defines a virtual organization as a network of geographically distant employees, who are linked by electronic communication and who perform most of their daily work at a distance (2003: 405-06).

[14] Dell provided in-person relations with its customers; telephone and internet purchasing, phone and online technical support, and next-day onsite support (Alberts et al., 2000: 43)

[15] Article 1 of the Frontex Regulation explains that it was established with task of “improving the integrated management of the external borders of the Member States.” In detail, this includes border control (checks and surveillance); detection and investigation of cross-border crime; the four-tier access control model—measures in third countries, cooperation with neighboring countries, border control, and control missions within the Schengen area; inter-agency cooperation; and coordination and coherence on actions at EU level (Marin, 2011: 135)

[16] For an illustration of this model, see Frontex, 2015: 14.

[17] EU developed the so called smart border system, an information sharing tool that share entry and exit data of migrant with to police and other law enforcement authorities across Member States to deter so called ‘overstayers’ (Schmitz, 2013).

[18] Hayes explains that the EU has developed a variety of technological instruments to support its border management, including drone planes, satellite surveillance systems, unmanned ground and marine vehicles, and combat robots (2010).

[19] Since 2013, drones, which are operated via geostationary satellites, are searching for refugees across the Mediterranean. EUROSUR has surveillance cooperation agreements with Mauretania, Morocco, Senegal, Gambia, Guinea-Bissau, and Cape Verde. It can monitor boats on the coats, trucks in the desert, and migrants via live screen in Warsaw (Grieger & Schlindwein, 2016).
[20] Neal highlights an interesting thought by Bigo with regard to Frontex' threat assessment. Bigo argues that the logic of threat is not necessarily one of response but one of anticipation and management. This entails a ‘proactive logic, which anticipates the risks and the threats, locating the potential adversaries even before they have any consciousness of being a threat to others.’ In other words, Frontex is assessing possible future threats that could emerge (Neal, 2009: 349).

[21] They are “composed of border guards from the EU Member States, experts in different areas of border management including land and sea border surveillance, dog handling, identification of false documents and second line activities such as establishing nationalities of irregular migrants detected at the border” (Frontex, 2017)

[22] They are able to handle a variety of problem areas: Land – Spanish NATO Rapid Deployable Corps (NRDC); Maritime – United Kingdom Maritime Force (UKMARFOR); Air – Italian Joint Force Air Component Command (JFAC); Special Operations – United States Special Operations Command Europe; Logistics – Joint Logistics Support Group (JLSG) from JFC Brunssum; Multinational Chemical Biological Radiological Nuclear (CBRN) Battalion led by Poland (NATO, 2016).

[23] As one of many examples, Frontex was involved in the so-called CLOSEYE project—collaborative evaluation of border surveillance technologies in maritime environment by pre-operational validation of innovative solutions—and given 9 million euros by EU’s security strand for the development and deployment of drones, satellites and aerostats over the Southern Mediterranean. The aim of this project is to give the EU a “operational and technical framework that increases situational awareness and improves the reaction capability of authorities surveying the external border of the EU (Marin, 2014: 13).


[26] Russia, Ukraine, Croatia, Moldova, Georgia, Macedonia, Serbia, Albania, Bosnia & Herzegovina, Montenegro, Belarus, Cape Verde, Nigeria, Armenia, and Turkey; and it started negotiations with Libya, Morocco, Senegal, Mauritania, Egypt, Tunisia, Brazil, and Azerbaijan (Kopp, 2012)