SOCIAL CONSTRUCTION OF SAFETY IN UAS TECHNOLOGY IN CONCRETE SETTINGS: SOME MILITARY CASES STUDIED

G.C.H. BAKX[1] & J.M. NYCE[2]
[1]Department of Military Behavioural Science & Philosophy,
Netherlands Defence Academy, Breda, The Netherlands.
[2]Department of Anthropology, Ball State University, Muncie, Indiana, USA.

ABSTRACT

Unmanned aerial systems (UASs) in general and UAS safety in particular have so far received little attention in the science, technology and society (STS) literature. This paper therefore reports on several (military) cases of this relatively new technology, focusing specifically on issues of safety. Quite often, safety of technology is considered the result of a rational process – one of a series of rational, often calculative, linear steps. The paper's results suggest that establishing safety in military UASs is very much a social process. Approaching (military) UAS safety from this perspective could perhaps be complementary to more analytical and rational perspectives on safety of this type of technology. Further research is therefore suggested on the implications that social processes can have for safety in UASs. So far, it seems, such a position on safety in technology has been little explored in both the STS and safety literature explicitly.

Keywords: military, safety, social process, social science, STS, technology, UAS.

1 INTRODUCTION

April 6 2011 two US servicemen were killed in the first (at least publicly acknowledged) drone friendly fire incident. An account of this tragic accident appeared in the Houston Chronicle October 15 2011 [1]:

> *Marine Staff Sergeant Jeremy Smith, 26, of Arlington, and Navy corpsman Benjamin Rast, 23, of Niles, Michigan, were killed by a Hellfire missile fired from a U.S. Predator drone in southern Afghanistan [Helmand Province] on April 6. Both men served in 1st Battalion, 23rd Marine Regiment, a Houston-based reserve unit, also known as The Lone Star Battalion. The Predator crew targeted Smith and Rast after mistaking their heat signatures on the drone's sensors for those of enemy forces, according to the 381-page redacted report obtained by the Houston Chronicle on Friday [but not officially released]. … Smith's father, Jerry Smith, said the images he saw from the drone's sensors were not clear. "It was one-inch long blobs," he said. "That's all you can see on their scope."*

This tragedy raises questions about UAS (unmanned aerial systems) safety, and also about how this is negotiated in concrete settings from development to the battlefield. For instance, if it is indeed the case that target representations were nothing more than one-inch blobs on a screen, as Jeremy Smith's father apparently was shown, then how could the Predator have been regarded a safe system to work with? How could such a target representation have been regarded as "workable" and reasonable by stakeholders throughout military UAS development, evaluation and system use? Questions such as these are important to ask. After all, current trends, at least in modern societies, have been to increase the development and fielding of unmanned combat systems. Given the Western military's increasing reliance on UAS,

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://journals.witpress.com
DOI: 10.2495/SAFE-V2-N3-227-241

issues like these require further study. The purpose of this paper is therefore to raise some scientific questions regarding this topic.

So far, UASs in general and the safety of UASs in particular have received little attention in the science, technology and society (STS) literature. This may be because this particular technology is relatively new. Another reason for this – and regarding military UASs in particular – could be that they have only recently been repurposed from a sole reconnaissance and surveillance platform for intelligence purposes into a weapon system as well. This is not to say that STS has not reported on military technological innovations. For example, Rappert et al. [2] provided an overview in 2008 on the development and dynamics of science, technology and the military within STS. STS research on military technology has also looked at the relationships between politics, society and cultural issues. Examples here are the use of science and technology for military purposes [3, 4] and the impact that (American) military research has had on the organization and institutions of science [5]. In STS, the development and use of military technology has generally been treated as the product of institutional and socio-political factors [6]. The emerging literature on the social construction of technology has brought in topics such as the "social shaping" of military technology [7] and the analysis of missile-guidance systems [8]. The topic of the social construction of safety in technology however, although touched on implicitly sometimes, does not really seem to be addressed in the STS literature. This paper will be, it is hoped, a contribution to the STS literature. Not just because it reports on a new technology, but because it demonstrates how useful an STS perspective can be when it comes to making analytical sense of what is built in platforms like UASs as assumptions and tacit understandings, especially regarding safety.

2 METHODOLOGY

What does safety mean when this is related to socio-technological concepts like UASs? With the help of the friendly fire incident described above and some other cases, the next section will consider this question. Socio-technological concepts will be understood in this paper as the whole of technology and its application, embedded in a structure of interdependent performing social actors and institutions, both operators and others. Throughout the paper therefore, any mention of military UAS, military UAS technology, or UAS and UAS technology in general, refers to (and implies) a particular socio-technological system taken as a whole, thus including both the technical and the sociological part unless when mentioned otherwise. After the first section, the second section will present a more in-depth analysis of military UASs as a social construction of relevant actors within boundaries of concrete settings. In this section, we will use terminology introduced by Wiebe Bijker [9], a classic in the constructivist studies of technology.

Cases are of course context-dependent and are thus of limited use for generalizations. Case studies however can expand and generalize theory [10], in this case the theory of safety in military UASs. It is not possible to treat all safety aspects of military UASs, no matter what method of analysis is used. Even more, it is not clear whether an exhaustive elaboration of all aspects of safety of military UASs would be possible anyways. We believe though that working towards "thick descriptions" of case material [11] can help us outline some of the critical issues related to safety and military UASs. Our aim therefore, was to study case material. Since we lacked access to data "from the inside" we mainly used open source material (mainly news sources), insights from the domain of safety, and insights from studies in naturalistic or concrete settings, to identify and define the UAS case material studied here. From there, we have used the STS-literature, with an emphasis on Bijker's

theory on the social construction of technology, as a tool through which we have evaluated the selected cases. By applying this part of the STS-literature to specifically issues of safety of a particular technology (in this paper the socio-technological system of military UAS) we have tried to extrapolate this theory towards something that we would define as the social construction of safety.

3 SAFETY OF MILITARY UAS: DOMAINS AND ASPECTS

Often safety is taken to be the same thing as numbers of injury, death or mechanical failures [12]. When approaching safety from this angle, safety – or the lack thereof – is in its most tangible form as the presence or absence of personal harm or technological breakdown. In socio-technological systems however, such as the UASs, it is the high-tech equipment and the social actors that, in conjunction with each other, yield these numerical features of safety. More to the point, these numbers are then seen as the inherent by-product of design and of establishing the system's final output. In short, from this point of view safety could be defined as those elements, or rather those interactions of elements, that amplify or dampen the mechanisms that ultimately lead to this personal harm or technological breakdown.

3.1 Military UAS safety domains

UAS engineers tend to focus on the possibility (and prevention) of technological breakdown. They focus on safety as the airworthiness of the aerial vehicle, i.e. the safety of the air vehicle itself and, indirectly, the safety of the people on the ground that could be hit if it crashes. Catalysed by the upcoming of non-military application of UASs, airworthiness efforts have been expanded recently to include the issue of how to integrate UASs into the (inter)national and commercial airspace system [13]. Safety from an engineering perspective thus broadened to include a concern for other aerial components. Currently, this results in a whole host of efforts directed on developing new technologies, enhanced reliability, procedures and standards in an attempt to handle this issue of military and civilian UAS safety.

Another safety domain of military UAS can be derived from the friendly fire case described above. In this case, safety – or again, the lack thereof – has expanded to include the well-being of friendly troopers. Obviously, some UASs have turned from "simple" reconnaissance and surveillance platforms into stand-off precision weapon systems, with intelligence collection as an additional task. Intelligence services (especially from the US and Israel) have exploited this capability extensively for the purpose of targeted assassinations of alleged terrorists [14]. In the military, however, a similar shift has taken place. In theory, UASs can perform any military task traditionally conducted by fighter aircraft and attack helicopters, ranging from precision killings and bombings, to the delivery of close air support for own and coalition ground troops. This shift for military UASs from reconnaissance and surveillance platforms to weapon systems has emphasized a concept of safety that includes third and other parties more than before. As the technology and its use changed and evolved, issues such as collateral damage and civilian victims – especially women and children – as well as the risk of victims among members of friendly forces, have become realistic safety concerns.

One safety domain related to military UAS is not an obvious one. Although UASs normally are referred to as unmanned systems, some prefer to call these systems "remotely operated" since, "although [they] do not carry humans on board … to control [them], skilled and coordinated work of [distant] operators … is required" [15]. The health of these operators, a recent study on US Air Force drone pilots suggests according to the New York Times [16], is an issue

of safety that needs to be explored. Obviously, degraded functioning of UAS operators could have consequences that are undesirable. The primary stressor here, according to the report, seems to be working long-hours and shift changes, necessary in order to keep the platforms in the air 24 hours a day. The report also suggests that some of the drone operators, due to the nature of their work, are developing post-traumatic stress disorders (PTSD). Since the extended functionality of the UAS as a distant weapon delivery platform is a relatively new development, it can place its operators in positions that are out of the ordinary; into the unknown. Issues that these operators confront with can thus be unfamiliar to even experts. Longitudinal data has yet to be collected on these kinds of distant war operations, especially from a "front row seat". Experience has been gained with warriors returning to their families after a day at war. For example, bomber crews for instance have operated from outside the operations theatre, sometimes from overseas, since at least WW II. A difference however is that these bomber crews, contrary to some of the UAS operators, do not see the effects of their work through magnifying glasses. It would seem then that occupational safety, in this case the physical and mental health of UAS operators, is another domain of safety that should be looked at, besides the safety of aerial vehicles, that of third parties, and that of friendly forces.

3.2 Aspects of safety of military UAS: the friendly fire case

At the surface the friendly fire incident described above seems to be a simple case of target confusion. When we look a little deeper however, a whole range of elements associated with military UASs and their deployment comes into view that, possibly in conjunction with each other, could have led to the mechanisms that enabled this target confusion. As has been suggested by the Houston Chronicle (quoted at the beginning of this paper), one contributing factor may have been some of the technological features that the drone operators had to deal with such as the quality of target representation: fuzzy blobs on a screen. Another factor could have been the numbers of actors such as a drone operator, analysts and a mission coordinator that apparently had to work together over long distances to get their weapons delivered half a world away. In absence of the official US Air Force report this analysis is based on what was written in the Portland Press Herald on November 9 2011 [17]:

> *The Air Force captain [at Creech Air Force Base in southern Nevada] angled his joystick and the drone veered toward the fighting taking place half a world away. … At the Air National Guard base in Indiana, [an] Air Force analyst watched the battle unfold on the drone's video feed. He sent … fragmentary reports to March Reserve Air Force Base in California, his communications link to the drone crew. … The analyst had doubts. "Disregard," he wrote, followed by "Not friendlies," followed by "unable to discern who pers[ons] are." … Receiving his message [at March Reserve Air Force Base], the mission intelligence coordinator and a trainee were dubious. … The trainee … didn't relay the information to the drone crew. … The Predator pilot was unaware of the analyst's doubts.*

What might have been another contributing factor is the chat-like communication apparently used during the incident. Again, according to the Portland Press Herald article [17]:

> *The analyst typed "3 friendlies in FOV," meaning three non-insurgents in the camera's field of view. A second later, he wrote "Pers[ons] are shooting W[est]," meaning they were firing west, away from the Marines on the road. … Almost immediately, the analyst had doubts. "Disregard," he wrote, followed by "Not friendlies," followed by "unable to*

discern who pers[ons] are." But he was certain of one thing: The shots were aimed away from the Marines. … [At March Reserve Air Force Base], the mission intelligence coordinator and a trainee were dubious. … As debate about the direction of the gunfire continued over the chat system, the analyst did not have access to radio traffic indicating a strike was imminent.

It would be unfair on the basis of this one case to attempt to draw any conclusions about the effectiveness (and role) that chat-like communication – with its short messages and weak contextuality – could have during high-consequence processes like this UAS weapon delivery. As far as we know the data is not simply there yet. In 2005 Nevile and Walker [18] pointed out that not much systematic research had been conducted on patterns of speech between individuals in professional settings, and little seems to have been changed since. It would also be unfair to make statements now about the apparent inferior quality of UAS imaging, or on the seemingly weaknesses in UAS command, control and communication infrastructures. What can be said though, is that features like these apparently could pose safety issues for military UASs because under certain circumstances they could ultimately lead to technological failure(s) or personal injury.

3.3 Aspects of safety of future military UAS: breaches in cyber space

The development of future military UAS has already begun. One current challenge in UAS technology and deployment that needs, without a doubt, further attention in the future, is security. On December 18 2009, the LA Times published this [19]:

Iraqi insurgents intercept live video feeds from Predator drones. Using a $26 program available on the Internet, militants were able to view raw footage, a breach discovered last year. … According to the Wall Street Journal, which first reported the intercepts Thursday, insurgents used a program called SkyGrabber, made by a Russian company for downloading music, photos and video from the Internet.

According to The Wall Street Journal, a person familiar with official reports on the incident said a day earlier that there was evidence that this was not a one-time event. Since the 1990s, when unarmed Predators were deployed in the Balkans, the Pentagon had known of this breach, one that opponents could exploit to intercept UAS video data streams. Also it is believed that certain states such as Iran train fighters how to do this. This interception flaw is however not the only cyber space breach in military UAS deployment. In 2011, the Predator and Reaper ground control stations have apparently been infected with a virus that, despite efforts to control it, affected ground control operations [20]. Also in 2011, another US drone, a RQ-170, was claimed to be hacked and landed in Iran [21]. These are cases that have appeared so far in the open literature. Whether there have been more such attacks against UASs is not really the issue here. What needs to be stressed instead is that cyber-events of this kind will increase in the future. What form or forms they will take is a difficult question to even predict. Singer, a Brookings Institution scholar and author of Wired for War, phrased the dilemma this way: "Robotic warfare is open-source warfare" [19]. Given the very nature of software, vulnerable to all kinds of disturbances and take-overs from the outside, especially when one's opponents include many Western trained computer sciences and engineers, who would argue against this?

Despite the obvious risks illustrated here, one could ask whether these cyber breaches should be considered as safety issues, as security issues, or as both. It can be argued that only

a thin line exists between security and safety, especially in the military. One for example could say that whenever a security breach occurs in the military, someone's life can be at stake. Soldiers or units can become victims of targeted attacks with improvised explosive devices (IEDs) if tactical information such as UAS reconnaissance data has been compromised. In similar ways, the well-being (and morale) of units can be at stake when (they believe) the objectives of their mission are known to enemy forces. These should be considered realistic threats, especially since cyber space activities have some typical characteristics, such as an independence of location, time and spatial distance. Furthermore, because more and more digital networks are connected to each other, events can get "coupled tightly" (sometimes without this being noted), thus having the potential to propagate quickly and increase in unpredictable unfortunate ways, sometimes exponentially [22]. The result is that what is often thought of as simply security breaches should be considered safety issues.

3.4 Safety: a fluid concept?

UAS engineers have derived much of their knowledge on safety from their manned counterparts. This has meant that much attention has been given to UAS airworthiness. Focus thereby is on establishing standards, normally followed by regulatory efforts, quality control and quality assurance. The result of this concern with classic safety control measures has been that safety is often equated with the reliability of individual components that then together constitute the socio-technological system of the UAS. Attention then thus far has been with the quality of vehicle and ground control station parts, and with establishing and upholding procedures for maintenance and for piloting vehicles safely. Framed this way, establishing safety of UASs seems to be a relatively simple, straightforward process, or at least one of predefined consecutive steps within a process that can be modelled and controlled.

The issues of safety that the cases presented here, however, are of quite a different order. They seem to belong to a more complex "anatomy" of safety, one that would be difficult to capture by rules, standards and segmentation alone. Perhaps, safety in actual settings could best be regarded a fluid concept, a concept that is difficult to regulate or control, because these actions depend ultimately on a subjective and momentary interpretation of what is to be regarded as both relevant and as facts. To represent targets as fuzzy one-inch blobs for instance was apparently regarded as safe by many before the friendly fire incident took place, or at least as sufficiently safe. This probably is no longer the case after the fact. Also, a network of operators, analysts and controllers is considered safe when its members manage to monitor and correct each other's actions. Such a network can however become a safety risk, when team members hold different, even conflicting, understandings of "the same thing". In similar ways, open-source technology can provide an advantage against an opponent because it can speed up innovation and change processes. Safety in concrete military UAS settings may not be possible by rule, mandate and establishing procedure(s) alone. At the same time however, this can make these systems more vulnerable for hackers.

Safety in concrete military UAS settings may not be possible by rule, mandate and establishing procedure(s) alone. It surpasses ideal types of modelled safety management on a regular basis, so it seems. Imagery designed for conducting surveillance tasks may prove to be of insufficient quality when used for precision weapon delivery. Safety here, this suggests, resides in the interplay between design, implementation and use. What this means is that, acknowledged or not, safety is an integral part of any design (technological, organizational or procedural) and of how this design is put into practice. The matter of the fact is that this is a

social process, informed and constrained as such. The design and fielding of UAS technology, including its aspects of safety, in other words, is a social construction. The next section will look into this.

4 SAFETY OF MILITARY UAS: SOCIAL CONSTRUCTION IN ACTUAL SETTINGS?

If it is indeed the case that safety resides in the interplay between design, application and use, then understanding how this works could be way to improve safety. In his book on the development of bicycles, Bakelite and bulbs, a classic in the constructivist studies of technology, Bijker [9] argued that technology gets constructed in the interplay between multiple "relevant social groups"; groups that, through their actions and understandings, in direct and indirect ways ultimately define the appearance and use of technology. What this means is that the development of technology, including its aspects of safety, would at least partially be a social process. The ideal type of safety management however, has known denominators and parallels thus largely a rationalistic decision making. Rationalistic decisions, after all, imply the availability and cognitive processing of all relevant knowledge and a subsequent objective weighing of all the possible alternatives by the decision maker(s) [23]. It is not clear whether in actual (or naturalistic) settings such objectivity is possible when dealing for example with safety of military UASs. Keeping Bijker in mind, let's look at this issue using the cases discussed before.

4.1 The friendly fire case

The friendly fire case offers much to consider when it comes to dealing with safety in actual settings. One issue of course is that of targeting imagery. From the Portland Press Herald of November 9 2011 [17]:

> *A firefight had broken out. Taliban insurgents had ambushed about two dozen Marines patrolling a bitterly contested road. The Air Force captain [at Creech Air Force Base in southern Nevada] … powered up two Hellfire missiles under [the drone's] wings and ordered a crew member responsible for operating the … cameras to search for enemy fighters. It didn't take long. Three figures, fuzzy blobs on the pilot's small black-and-white screen, lay in a poppy field near the road. "Hey now, wait. Standby on these," the pilot cautioned. "They could be animals in the field."*

The UAS operators obviously had to deal with inferior imaging technology. One-inch blobs that could be animals in the field are not exactly the kind of representation or symbology one would expect to find in high-tech equipment such as a Predator. In today's world of high-definition television, there must have however been good reasons to accept this kind of representation as sufficiently safe for weapon delivery. After all, it must be assumed that the Predator system would not have been developed in ways that potentially would be unsafe for one's own troops. How is it then that such a targeting imagery came to be regarded as "workable" by stakeholders during military UAS development, evaluation and use? Was this because the Predator imaging technology sufficed for the earlier reconnaissance tasks? This friendly fire incident, however, is not the only incident that involves target imagery. It closely resembles another deadly mistake involving close air support with a Predator. In early 2009 at least 15 Afghan civilians were killed after a Predator crew mistook them for Taliban preparing to attack a US Special Forces unit. In this latter case, analysts, located at Air Force Special Operations Command in Florida, also had doubts about the target's identity. Their warnings

that children were present were disregarded by the drone operator and an Army captain who authorized the airstrike. If these limitations of this technology have been exposed before, did this issue then lack traction? And if so, why would this have been? When exploring how safety gets established in actual settings, these are the kinds of questions that need to be answered.

Another issue to be looked at more closely in the friendly fire case concerns the command and communication format and infrastructure in which the incident took place. Procedural check-ups apparently were part of the target acquisition and weapons delivery process. An intelligence data analyst in Indiana checked the drone's video streams and communicated his assessments through a coordinator team in California to the drone pilots at the UAS ground control station in Nevada. While on the one hand procedural checking seems a wise and obvious thing to do when delivering weapons half a world away, it also makes one wonder why such procedural checks are necessary at all in apparent safe systems. Are systems of this type themselves that weak that they need multiple double checks? And if so, why is then a chat-like form of communication used for coordination in high-consequence missions like the one described here? Is this for technical reasons? Is it because the Predator originally had been developed and equipped for reconnaissance flights? Have communication channel(s) and the infrastructure used today for UAS target acquisitions and weapon deliveries at all been the result of some conscious deliberation of alternatives? Or did it rather emerge from UAS technology (and missions) in place at the time?

It would be unwise, based on two cases, to argue that the information structure used during the friendly fire incident is a failure. Still, it could be valuable to take a closer look into the processes and factors from which both designers' and users' commitments to such communication structures emerged. Such a study could provide a more complete understanding of how conceptions of safety, at least in regard to military UASs, come about.

4.2 The interception case

A similar analysis can be performed on the interception case. Should, for instance, the interception of drone video streams by Iraqi insurgents in 2009 be attributed to "laziness and arrogance", as was stated in the LA Times on December 18 2009 [19]:

> *P.W. Singer, author of "Wired for War" and a scholar at the Brookings Institution, … said insurgents' interceptions of video feeds are, in part, a result of "laziness and arrogance" by the Pentagon, which didn't encrypt the unmanned systems because officials assumed militants wouldn't be able to figure out how to intercept them. Singer said the Pentagon knew about the problem in the mid-1990s, when unarmed Predators were used in the Balkans conflict. Hackers in Eastern Europe were able to intercept Predator video feeds, he said – but complained that they were unable to intercept encrypted feeds of the Disney Channel.*

Could it be that simple, that laziness and arrogance were at the heart of this? Or is there more that needs to be added to this discussion? Could there have been other rationales behind this? As has been argued with the friendly fire case, UAS technology and its safety can ultimately be regarded as social constructs. Could it be, for instance, that indications from the intelligence sources were such that opposing forces, organized or acting as individuals, were not seen as being able to exploit flaws in system design so that own or coalition forces would be in real danger, as was suggested in the Wall Street Journal [24]? Could it be that the voices of intelligence specialists got more traction in today's environment in which development and implement costs

for military technology both have risen and are under increased scrutiny? Perhaps, chances of opponents exploiting Predator technologies were not regarded enough to outweigh the costs needed to secure the data streams, especially since some would believe that they, even when able to intercept this type of data, would remain exempted from the further operational decision process anyhow. Or perhaps these voices would have lacked traction anyways because the enemy may be able to gain the same information through other design flaws? There may be more macro-level issues involved here too. In the United States, and probably also elsewhere in the Western world, Predator attacks are seen as a triumph of Western science and technology. This is because by many they are considered as accurate and relatively humane (because of its pinpoint kill-zones), and because the effects of these attacks seem so easy to measure [25]. Has this led us to underestimate the potential that opponents have, to exploit and turn to their advantage our own technologies [26]? Questions such as these have been informed by what is going on at this time in the military UAS industry as derived from open source material. Answering these questions, however, is beyond the scope of this paper. What these questions do bring to mind though is that the notions of those who are directly involved in system design and system application can be affected by how they see others in this process. The interaction between opponents regarding the perceptions each holds of the other's technology and military competence for instance also figures in here. What this means is that not only technological processes and its safety "markers" can be regarded as social constructs. Stakeholders and other actors in the process, as far as they inform design and implementation, even indirectly, can be considered such as well.

This interception case brings up another issue. Evidence suggests that there has been a trend in the past decennia for military organizations to shift from in-house development and innovation to buying ready-made or ready-to-be-adapted available products. These are often referred to as commercial off-the-shelf (COTS) technology. The Dutch Minister of Defence for instance ordered this in his policy letter of April 8 2011, as a result of severe budget cuts [27]. After the 2008 worldwide financial crisis, he said, any equipment to be bought for future use in the Dutch Armed Forces, has to be purchased either commercially or military off-the-shelf (COTS or MOTS). Exceptions will be made only rarely, he concluded. This has been the case too for simulator technology within the Royal Armed Forces of the UK [28]. Industries like the gaming industry invest so much money that it would be impossible with current defence budgets to start innovation projects that could compete with these industries. There has also been, for the same reason, an increase in the military use of open-source software and technology, perhaps without even realizing some of the security and safety issues embedded in how these technologies are developed. Also, there is the increased demand for interconnectedness and interoperability in national and international military theatres. Another worldwide trend is that life-cycles of technological products have shortened over time. The effect that these developments, especially when working in parallel, could have on the development of military UAS technology and its broader operational concepts, is that safety issues are not given the hearing they deserve. Perhaps the interception of video data streams and last year's virus-infection of the Predator and Reaper UAS ground control station software could in part be the result of these developments?

4.3 A Bijkerian inspired reconnaissance

What these cases illustrate is that establishing safety – or the lack thereof – of military UASs in concrete settings is not a straightforward linear process. The friendly fire case for instance seems to confirm Bijker's argument that technology is constructed through the interplay of

notions and activities of social groups [9]. Many stakeholders seem to be involved in the processes of military UAS design and application. Engineers, military commanders, analysts, end-users, but also for instance the public have their own perspectives, inputs and needs. It seems as if their goals and demands all have to be balanced against each other at the same time. How else could we for instance have proceeded from using the Predator system as a surveillance tool to using the very same system as a remote weapon delivery platform providing close air support?

This shift in UAS application could be understood through Bijker's concept of "interpretative flexibility", the variety of meanings that could be attributed to a certain artefact. After all, without the ability to visualize (or conceptualize) a reconnaissance platform as a tool for weapon delivery, it would have been impossible that this shift could have been made at all. The attribution of meaning to artefacts seems limitless at first. But as Bijker pointed out, "attributions of meaning are social processes and [are], as such, … bound by constraints. Previous meaning attributions", he argues, "limit the flexibility of later ones" [9]. The issue of imaging technology and the communication structure used in the friendly fire case can be seen in this way. Both these issues suggest that the Predator technology and its application were built on notions of what was already there; the tools and procedures were designed and optimized for reconnaissance. That establishing safety of military UASs is a social process and therefore inherently informed and bound by these constraints, seems to be confirmed here. What the friendly fire case also seems to suggest is that – in turn – the Predator, its current technology and its operational concepts, are defined by this reality. Social actors and socio-technological concepts are inextricably linked; the one informs the other.

Stakeholders, at the same time, can differ from each other with respect to their proximity to the design and utilization of military UAS. Some affect these processes directly, others in more indirect ways. While Bijker pays little attention to these latter ones (e.g. consumers), with UAS technology these "extended" stakeholders such as opponents inform, through their actions and non-actions, the perception of designers and other stakeholders that are more directly involved. One's opponents' actions and influences therefore do need to be taken into account when analyzing how concepts of military UAS and deployment and related issues of safety come about. Even more, the perception held of one's adversaries should be incorporated in any analysis of UAS technology. After all, the social construction of opponents by those directly involved (like the social construction of customers by engineers and industries in Bijker's cases) can affect their perception of what will "work" and what certainly not. If one's understanding of the opponents' understanding of UAS technology, their role in warfare, and their competence regarding countermeasures, is not very accurate, this can have any number of unanticipated results.

It is necessary to return to the influence that current technology and its operational concepts can have on how stakeholders understand this and future technology and their related operational concepts. Bijker introduced the concept "technological frame". This concept can be associated with for instance mental models, organized knowledge structures [29], or with what Thomas Kuhn [30] referred to as a scientific paradigm. A technological frame comprises all those elements of the technical artefact, from material and technical to social and cognitive, "that influence the interactions within relevant social groups and lead to the attribution of meanings to technical artefacts". Examples of such elements are accepted theories, tacit knowledge, design methods and design criteria. In Bijker's analysis in 1997, these technological frames were seen as relatively distinctive and stable ones, thereby providing fertile grounds for standardization efforts. Modern digital technology however, it could be argued,

has quite possibly altered the landscape in which current and future military UASs are to be developed and brought into practice. Today's digital technologies, by enabling swing-role capabilities, customized options and easier updates, can lead to more hybrid technological frames with diffused boundaries and relatively lower product life-cycles. The adaptability and flexibility that follows from this, once it has become the new norm, could give rise to even more hybridity as can be seen when comparing today's smartphones to the first generation mobile phones. Although such processes can lead to great opportunities for the range of applications to be covered, at the same time it implies less opportunities for standardization efforts to succeed.

One problem with Bijker's theoretical frame for the social construction of technology is that it is constituted by more or less static and distinctive concepts such as the concept of "technological frames". Also, it presumes relatively stable, fairly easy to identify, social groups that tend to have almost binary roles (higher or lower "inclusions") in these frames. Less attention is given by Bijker to the dynamics of process; on how for instance, social groups become relevant ones, and why the traction of their messages has the value that it has. For example, digital technology has enabled the creation of readily available technology and shorter lifespans for products, thus increasing profits. It has also redefined and reallocated where expertise is located and defined. In some sectors, digital technology has even changed the power dynamics between the defence forces and other stakeholders in the development of military systems. An example of this is the case of simulator technology mentioned earlier. Stakeholders and current technology apparently are more than inextricably linked; the one seems to bring forth the other.

5 DISCUSSION

The paper raises some questions on how aspects of safety regarding military UAS technology come about in concrete (or actual or naturalistic) settings. As has been argued, ideal types of safety management, resting on assumptions of objectivity and rationality, are not sufficient, at least for some of the safety issues in the cases presented here. In this paper, several cases on military UAS technology have been taken from the real world and their aspects of safety identified. Establishing safety in these concrete settings appeared to be a social process with many stakeholders, all with their own perspectives, knowledge, capacities, inputs and demands. Safety in military technological concepts such as UASs, it can be argued, is a social construction, informed and constrained as this can be by social mechanisms and processes. Establishing safety in UAS technology, in short, can be regarded a social process as opposed to, or rather in addition to, a mere technical rationally calculative one. If this indeed is the case, then understanding how this works could help establish more comprehensive analytical foresight and hindsight opinions on (aspects of) safety related to socio-technological concepts such as military UASs.

The social sciences have long acknowledged the shortcomings of rationality in actual settings [31]. The establishment of scientific domains such as intuitive (or naturalistic) decision-making has been the result of this [32]. The social sciences however do not stand alone here. The bounded rationality of social actors, especially when facing risks, has been pointed out by Kahneman and Tversky in a research program that ranged from 1937 till 1996. The results of this program have been recognized even in such domains as economics in which the notion of rational actors has long been fundamental for theory development [33]. Organizational decision-making research has also focused on what decision makers actually do, as defined by their organizational and real-world context [34]. Scholars from philosophy

further called attention to the "normative aspects of safety and risk" because of which estimates of these concepts will by definition be value-loaded [35]. Currently, the field of quantum physics is mentioned sometimes as a method to tackle this issue of non-rationality in social contexts. Although we would embrace any kind of theoretical examination from the natural sciences that could help to bridge the existing gap between the natural and social sciences, we believe that in the cases discussed here, to understand the social dynamics and the issue of non-overall rationality, the best available frame of analysis is that which has emerged from the STS literature.

What the analyses presented here suggest is that social actors and socio-technological concepts are inextricably linked and that together they constitute the reality in which technological innovation, development and fielding of military UAS technology occurs. In brief, it seems as if both help to construct the other. Social actors obviously construct technology and its broader operational concepts. At the same time, technology seems to enable one network of social actors above others. This would have to be a process of social construction again. After all, technology by itself can not initiate anything. The question here is: How does a current technology, through the understandings and actions of social actors, help to add others to the network of social groups, and how would the relevancy, or traction, of these social actors be established? This would be an item to pick up for further research on safety of military UAS technology since each player in the network has the ability in one way or another to add their own perspective to the construction of safety. More in general, one could ask whether regarding establishing safety in military UAS technology as a social or sociological process could add to the quality of our foresight and hindsight opinions of safety of this type of technology.

"The STS literature, as we have pointed out at the beginning of this paper, does not say much about military UASs at all, and even less about UAS safety issues. The safety literature on UASs, above all, seems to be dominated by a technocratic and engineering approach, covering issues such as airworthiness, regulations, requirements and licensing [36–41], machine autonomy [e.g. 38, 42], and sense-(or detect-)and-avoid technology [39, 43, 44]. Social aspects of UAS safety do get addressed in human factors literature. However, it is mainly empiricist positivist micro-level cognitive issues such as situational awareness and its related aspects of human-machine interfacing [38, 39, 45] that get attention in this literature. Social aspects of risk have of course been addressed in the past [46, 47]. Risk and safety have even been considered a social construction sometimes [12, 35, 48, 49]. The establishment of safety of technology in general however, and of military UAS safety in particular, is in STS and safety literature normally not considered a social process explicitly, leaving the ramifications and implications of this unknown. Answering questions like the ones above would therefore add to the STS and safety literature.

6 CONCLUSIONS

The literature on UAS safety, civilian and military, has so far been dominated by engineering (technological) and regulatory perspectives. This paper attempts a correction of this by noting that, to make analytical sense of issues of safety with this kind of technology, we need to proceed beyond these conventional means of dealing with safety. Some cases on military UAS have been evaluated and demonstrate that this "turn" makes some sense, at least with the kind of data that we had access to. What the evaluation of these cases suggests is that safety in military UAS technology is not only a case of technology, of setting standards, and of enforcing rules, but that underpinning and alongside this, safety of military UAS technology is also

informed and constrained by a whole set of social dynamics. Safety in military UAS, is therefore not only "built in", i.e. engineered, managed, and enforced, but also includes for instance assumptions and tacit understandings of various stakeholders involved in the design, implementation and use of UASs. Safety of military UASs, in short, is above all a socially constructed phenomenon. This paper has demonstrated there is sufficient rationale to perform further studies on UASs from this perspective. If one takes this angle, this can provide us with valuable insights on UAS safety issues – ones which current engineering and regulatory approaches have left so far unexplored. This would also help us understand the military and the UAS industrial practices in which UAS safety is embedded. Further, pursuing studies like these can add to the empirical and analytical diversity that is one of STS's strengths.

REFERENCES

[1] Wise, L., Confusion blamed in drone strike killing 2 in Houston unit. *Houston Chronicle*, Available at http://www.chron.com/default/article/Confusion-blamed-in-drone-strike-killing-2-in-2219732.php#page-2, 15 October 2011 (accessed 14 January 2012).

[2] Rappert, B., Balmer, B. & Stone, J., Science, technology and the military: priorities, preoccupations and possibilities. *The Handbook of Science and Technology Studies*, MIT Press: London, 2008.

[3] McNeill, W.H., *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*, University of Chicago Press: 1982.

[4] Creveld, van, M. L., *Technology and War. From 2000BC to Present*, The Free Press: New York, 1991.

[5] Forman, P., Behind quantum electronics: national security as a basis for physical research in the United States, 1940-1960. *Historical Studies in the Physical and Biological Sciences,* **18(1)**, pp. 149-229, 1987.

[6] Sapolsky, H.M., Science, technology, and military policy. Science Policy Studies in Perspective, eds. I. Spiegel-Rosing & D. De Solla Price, London: Sage Publications, 1977.

[7] MacKenzie, D. & Wajcman, J., *The Social Shaping of Technology*, 2nd edn. Open University Press: Berkshire, 1999.

[8] MacKenzie, D., *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*, MIT Press: Massachusetts, 1990.

[9] Bijker, W.E., *Of Bicycles, Bakelites, and Bulbs*. The MIT Press: Cambridge, 1997.

[10] Yin, R.K., *Case Study Research. Design and Methods*, 4th edn. SAGE Publications: Thousand Oaks, 2012.

[11] Geertz, C., *The Interpretation of Cultures: Selected Essays*, Basic Books: New York, 1973.

[12] Slovic, P., Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield. *Risk Analysis*, **19(4)**, pp. 689–701, 1999. doi: http://dx.doi.org/10.1111/j.1539-6924.1999.tb00439.x

[13] Ramalingam, K., Kalawsky, R. & Noonan, C., Integration of Unmanned Aircraft System (UAS) in non-segregated airspace: A complex systems of systems problem. *Systems Conference, 2011 5th Annual IEEE*, pp. 448–455, 2011.

[14] Mayer, J., The predator war. What are the risks of the C.I.A.'s covert drone program? *NewYorker*, available at http://www.newyorker.com/reporting/2009/10/26/091026fa_fact_mayer, 26 October 2009 (accessed 14 January 2012).

[15] Salas, E., *Human Factors of Remotely Operated Vehicles: Advances in Human Performance and Cognitive Engineering Research*, Elsevier: Amsterdam, 2006.

[16] Bumiller, E., Air Force done operators report high levels of stress. *New York Times*, available at http://www.nytimes.com/2011/12/19/world/asia/air-force-drone-operators-show-high-levels-of-stress.html 18 December 2011 (accessed 26 December 2011)
[17] Cloud, D.S. & Zucchino, D., In focus: Drone on trial after marines killed. Safeguards are in place, but the fog of war is still a factor. *Portland Press Herald*, available at http://www.pressherald.com/news/nationworld/Drones-on-trial-after-Marines-killed_2011-11-09.html, 9 November 2011 (accessed 9 December 2011).
[18] Nevile, M. & Walker, M.B., *A Context for Error. Using Conversation Analysis to Represent and Analyse Recorded Voice Data* (Rep. No. B2005/0108). Australian Transport Safety Bureau (ATSB), 2005.
[19] Zucchino, D. & Barnes, J.E., Iraqi insurgents intercept live video feeds from Predator drones. *Los Angeles Times*, available at http://articles.latimes.com/2009/dec/18/nation/la-na-drones18-2009dec18, 18 December 2009 (accessed 10 December 2011).
[20] Air Force Space Command Public Affairs, *Flying Operations of RremotelyPiloted Aircraft Unaffected by Malware*, available at http://www.afspc.af.mil/news1/story.asp?id=123275647, 2011 (accessed 22 March 2012).
[21] BBC News Middle East, Iran shows film of captured US drone. *BBC News*, available at http://www.bbc.co.uk/news/world-middle-east-16098562, 8 December 2011 (accessed 22 March 2012).
[22] Perrow, C., *Normal Accidents*, Princeton University Press: Princeton, 1999.
[23] Simon, H.A., Rational Decision-Making in Business Organizations. *Nobel Memorial Lecture*, 1978.
[24] Gorman, S., Dreazen, Y.J. & Cole, A., Insurgents hack U.S. drones. $26 software is used to breach key weapons in Iraq; Iranian backing suspected. *Wall Street Journal*, available at http://online.wsj.com/article/SB126102247889095011.html, 17 December 2009 (accessed 10 December 2011).
[25] Schmitt, E. & Dao. J., Use of pinpoint air power comes of age in new war. New York Times, available at http://www.nytimes.com/2001/12/24/international/24WEAP.html?scp=1&sq=schmitt%20dao&st=cse, 24 December 2001 (accessed 30 January 2012).
[26] Nyce, J.M. & Dekker, S.W.A., IED casualties mask the real problem: It's us. *Small Wars & Insurgencies*, **21(2)**, pp. 409–413, 2012. doi: http://dx.doi.org/10.1080/09592318.2010.481493
[27] Dutch Minister of Defense, Defensie na de kredietcrisis: Een kleinere krijgsmacht in een onrustige wereld, *Policy Letter*, 8 April 2011.
[28] Hughes, J., British military updating war simulators to keep up with XBox games. *Digitaltrends*, available at http://www.digitaltrends.com/gaming/british-military-updating-war-simulators-to-keep-up-with-xbox-games, 29 December 2011 (accessed 01 January 2012).
[29] Mathieu, J.E., Heffner, T.S., Goodwin, G.F., Salas, E. & Cannon-Bowers, J.A., The influence of shared mental models on team process and performance. *Journal of Applied Psychology*, **85(2)**, pp. 273–283, 2000. doi: http://dx.doi.org/10.1037/0021-9010.85.2.273
[30] Kuhn, T.S., *The Structure of Scientific Revolutions*. Chicago: The University of Chicago Press: Chicago, 1996[1962].
[31] Simon, H.A., A behavioral model of rational choice. *The Quarterly Journal of Economics,* **69(1)**, pp. 99–118, 1995. doi: http://dx.doi.org/10.2307/1884852
[32] Klein, G., *Sources of Power, How People Make Decisions*, Massachusetts Institute of Technology: Cambridge, 1999.
[33] Kahneman, D., Maps of bounded rationality: Psychology for behavioral economics. *The American Economic Review,* **93(5)**, pp. 1449–1475, 2003.

[34] Shapira, Z., (1997) as cited in Lipshitz, R., Klein, G., & Carroll, J.S., Introduction to the special issue. Naturalistic decision making and organizational decision making: Exploring the intersections. *Organization Studies*, **27(7)**, pp. 917–923, 2006.
[35] Moller, N., The concepts of safety and risk. Handbook of Risk Theory, eds. S. Roeser, R. Hillerbrans, P. Sandin & M. Peterson, Springer: Dordrecht, pp. 55–85, 2012. doi: http://dx.doi.org/10.1007/978-94-007-1433-5_3
[36] Cork, L., Clothier, R., Gonzales, L. F. & Walker, R., The future of UAS: standards, regulations, and operational experiences. *IEEE A&E Systems Magazine*, pp. 29–44, 2007.
[37] Dalamagkidis, K., Valavanis, K.P. & Piegl, L.A., Current status and future perspectives for unmanned aircraft system operations in the US. *Journal of Intelligent and Robotics Systems,* **52(2)**, pp. 313–329, 2008. doi: http://dx.doi.org/10.1007/s10846-008-9213-x
[38] European Aviation Safety Agency (EASA), *Policy Statement Airworthiness Certification of Unmanned Aircraft Systems (UAS)* (Doc. No. E.Y0013-01), 2009.
[39] Hobbs, A., Unmanned aircraft systems. *Human Factors in Aviation*, eds E.Salas & D. Maurino, Elsevier Inc: Burlington, 2010.
[40] Eurocontrol, *Unmanned Aircraft Systems - ATM Collision Avoidance Requirements* (Rep. No. CND/CoE/CNS/09-156), 2010.
[41] United Sates Air Force Scientific Advisory Board, Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare (Rep. No. SAB-TR-10-03), 2011.
[42] United Sates Air Force Scientific Advisory Board, *Operating Nex-Generation Remotely Piloted Aircraft for Irregular Warfare* (Rep. No. SAB-TR-10-03), 2011.
[43] Eurocontrol, *Eurocontrol Specifications for the Use of Military Unmanned Aerial Vehicles as Operational Air Traffic Outside Segregated Airspace*, (Doc. No. EURONCONTROL-SPEC-0102), 2007.
[44] NATO Joint Capability Group on Unmanned Aerial Vehicle (JCGUAV), *Sense and Avoid Requirements for Unmanned Aerial Vehicle Systems Operating in Non-Segregated Airspace* (Rep. No. AC/141(JGCUAV)N(2012)0002). NATO Naval Armaments Group, 2012.
[45] Williams, K.W., *Human Factors Implications of Unmanned Aircraft Accidents: Flight-Control Problems* (Rep. No. DOT/FAA/AM-06/8). Federal Aviation Administration Office of Aerospace Medicine: Washington DC, 2006.
[46] Douglas, M. & Wildavsky, A., *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*, University of California Press: Berkeley, 1982.
[47] Johnson, B.B. & Covello, V.T., *The Social and Cultural Construction of Risk: Essays on Risk Selection and Perception*, Reidel Publishing Company: Dordrecht, 1987.
[48] Turner, N. & Tennant, S.J., As far as is reasonably practicable: socially constructing risk, safety, and accidents in military operations. *Journal of Business Ethics*, **91(1)**, pp. 21–33, 2009. doi: http://dx.doi.org/10.1007/s10551-009-0065-5
[49] Turner, N. & Gray, G.C., Socially constructing safety. *Human Relations*, **62(9)**, pp. 1259–1266, 2009. doi: http://dx.doi.org/10.1177/0018726709339863