Privacy on the Battlefield? Ethical Issues of Emerging Military ICTs

J. Sigholm
Dept. of Military Studies
Swedish National Defence College
Box 27805, SE-11593 Stockholm, Sweden
johan.sigholm@fhs.se

D. Andersson
Div. of Information Systems
Swedish Defence Research Agency
Box 1165, SE-58111 Linköping, Sweden
dennis.andersson@foi.se

Abstract

Privacy on the battlefield? A bizarre thought at first glance – but is it really that far-fetched? In this study we look at modern conflicts, such as the war on terror, and dig deeper into what privacy means to a soldier engaged in such a campaign. With the ever-increasing amount of technology used for troop command and control, there is less room for an individual soldier to act without being watched. An open question is how the soldiers will react to all this surveillance. It is a long established fact that excessive workplace surveillance may result in negative performance consequences for the affected employees. We believe it is fair to raise the same question about emerging technology for the modern battlefield, and to critically assess this technology from a privacy perspective. Our study does not reveal any hard evidence of ongoing privacy violations, nor of the actual significance of privacy in modern warfare. We do however provide a model for studying how soldier performance relates to the fulfillment of various needs, and examine where attributes such as privacy fits in to the equation. We also call for the research community to pick up the thread and conduct empirical studies on the matter.

Keywords: Battlefield, privacy, military, ICT, C2, PET, surveillance, performance

INTRODUCTION

Following the 9/11 2001 terror attacks in New York and Washington D.C., the U.S. significantly strengthened its security procedures, within sectors such as transportation and critical infrastructure. Legislation such as the Patriot Act (2001) has given departments and agencies from the federal government a broadened mandate to gather citizen data, such as by use of video surveillance or by monitoring of private voice and data communication (Ball, 2004). However, these actions have not been without controversy. A hot debate of the balance between the needs for societal security and individual privacy has been ongoing in parallel (Rotenberg, 2007; Wright, 2008; Bajoria, 2010), and many critics have pointed out that excessive security measures threaten to severely limit civil liberties, such as privacy. In Europe the development has been similar, but perhaps a bit slower (Bigo, Shapiro and Fedorov, 2004). Although countries like UK, Spain and Sweden have also been targeted by terror attacks (Richburg, 2004; Left and Oliver, 2005; Jamieson, 2010), many smaller countries still do not

regard similar acts of violence within their borders as a plausible threat. While common laws such as the Data Retention Directive (European Parliament, 2006) have been passed within the EU community as a reaction, these have been highly controversial and politically sensitive. For instance, Sweden has still not implemented the directive into national legislation even though the final deadline was in 2007 (Ricknäs, 2011), preferring heavy fines and trial by the European Court of Justice (European Commission, 2011) to risking a storm of opinions like the ones created by the passing of the controversial FRA signals intelligence law of 2008 and the implementation of the anti-piracy IPRED EU directive of 2009 (Deibert, Palfrey, Rafal and Zittrain, 2010). The hot debate on privacy versus security has also resulted in the formation of new privacy-advocating political parties, some of which have gained seats in national parliaments as well as the European Parliament (Kravets, 2009).

The December 11 2010 suicide bombings in central Stockholm (Jamieson, 2010), and the narrowly thwarted terror attack against a Danish newspaper following Christmas a few weeks later (Sandels and Stobart, 2010) have made the issue of anti-terrorism countermeasures a medial and political hot topic. Citizens of these countries have started to realize that they are not immune to the events in the surrounding world and according to recent polls the acceptance rate for government surveillance of private communication, such as Facebook, has increased to exceptionally high levels. Among young people in Sweden, including those in relevant ages for becoming military recruits, there is an 85 % acceptance rate of video surveillance aiming to prevent serious crime, and a 74 % acceptance rate of general Internet monitoring with the goal of preventing acts of terrorism (Pernemalm and Lindgren, 2011). This stands in contrast to previous studies (Tavani, 2008; Nissenbaum, 2005) that have shown the importance of privacy to the individual and society alike.

However, the general opinion on privacy seems to vary with context; for instance in workplaces and public areas the need for privacy is generally considered lower than it is in private homes, and it is also recognized that some work forces, such as the police, are expected to endure a higher infringement on their privacy (Miller, 2005). As previously noted by Schneier (2008), this may not come as a surprise. As a result many communities have come to accept, and even expect, a high degree of surveillance, even at times when they are not fully certain of its existence. Still, it is apparent that there is a limit to the level of monitoring they will accept, which became obvious after the announcement of the 'iPhone tracker bug' (Allen and Warden, 2011) which launched a massive unrest among users worldwide, and received lots of media attention for a short while. While Google-sponsored mobile operating system Android was accused of the same privacy infringement (Eriksson, 2011), it got off the hook easier since it informed the user about the data collection and provided an opt-out option (Fried, 2011). This could be considered a sort of informed consent, although Malek (2005) would probably not agree that the consent the users were asked to give was completely informed.

In the military, the command and control (C2) capability has increasingly come to rely on the use of potentially privacy-infringing Information and Communication Technologies (ICT) such as Blue Force Tracking (i.e. keeping track of friendly forces and assets), health monitoring and video feeds. These systems are designed to increase troop performance. A question that has not received very much attention though is that of what level of privacy infringement it causes; How much more surveillance can the society demand that soldiers accept before the lack of privacy becomes a problem? Is it perhaps already a problem?

BACKGROUND

Security technology, especially related to ICT, has become increasingly important during the last decade, contributing to the global struggle against environmental threats, cross-border organized crime, currency speculation, pandemic diseases and terrorism. This paper focuses on emerging ICT for the defense sector, and how it may come to change conditions for professionals tasked with protecting our society from various threats. The paper's contributions are mainly the identification of some unforeseen ethical and possibly economic drawbacks which may arise from the ongoing converging and networking of military ICT systems, the recognition and analysis of the complexity of the multi-context

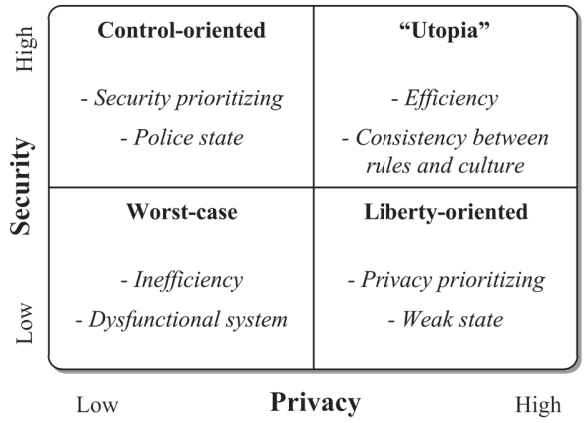

Figure 1. The relation between privacy and security in the context of a military operation. The cell labels describe the main orientation of the operation and attributes illustrate characteristics.

battlefield workplace and the proposed concept of applying privacy enhancing technologies in future defense ICT systems in order to avoid or mitigate the effects of the anticipated ethical pitfalls. To highlight and exemplify some of the challenges that lay ahead we use the case of emerging technology within military voice-and-data radio communications systems. These systems, such as the U.S. Joint Tactical Radio System (*JTRS*), based on mobile infrastructure-less ad-hoc networking, represent state-of-the-art technology within its area, are likely to be the dominant military communications technology within 10-15 years (Sigholm, 2010; Howard, 2010; Woo, 2008). Further down in this paper, we will investigate the JTRS system and two military application services that use ICTs to communicate with the surrounding world.

Although the debate of security versus privacy has been accused of sidetracking the discussion from the more important issue of safeguarding society against threats of tyranny and terror (Granick, 2006), as well as having received critique for being a completely false debate (Schneier, 2008), it may still be relevant for our causes to put them in relation. In this way we can try to identify the main characteristics of having, or lacking, security or privacy in the context of a military operation. Figure 1 shows the relation between privacy and security in the context of a military operation, and the cell labels describe the main orientation of the operation and attributes illustrate characteristics. As we can see, there are several opposing attributes, where the worst-case represents a dysfunctional system where both levels of security and privacy are low. The utopian scenario, where security and privacy are strong, is characterized by efficiency and consistency between rules and culture. This should reasonably be the goal of every military operation, although traditional military operations are perhaps more likely to fall under the control-oriented category. In order to make a move towards the upper right hand of the figure, we need to analyze the meaning of privacy and its relevance in a military context.

One of the oldest known definitions of privacy is that of Warren and Brandeis (1890), commonly cited as 'the right to be let alone'. This definition is valid in many contexts, but for this study it is not sufficient. Surely we cannot accept soldiers to demand the right to be let alone at all times. Possibly it could be applied during off-duty time, but even that is questionable. Instead we turn to Aiello and Klob (1996) who define privacy as 'the ability for an individual to control the use of their own personal data, wherever it may be recorded'. This definition seems to suite well with the domain of our study and corresponds to a need that the soldier on a battlefield might still want to have fulfilled. The matter of privacy becomes even more interesting once soldiers become subject of surveillance and monitoring, such as can be expected from emerging ICTs supporting advanced C2 systems.

To investigate what privacy problems the ICTs might infer on the battlefield we first turn to research on workplace surveillance. Workplace surveillance has existed since the beginning of the industrial

revolution and is predominantly used by the employer to verify that the employees carry out their assigned tasks. Technology progression has made modern workplace surveillance more effective and easier to perform, and it also allows for higher levels of detail. This has led to many cases where employees have experienced that their personal privacy has been invaded, which in turn had a negative effect on their performance, such as reduction of employee self-esteem and creativity (Kizza and Ssanyu, 2005). However, when it comes to certain employee categories, such as first responders, military or crisis management, there are still many questions to be answered. In the military, especially during field duty, the soldier may find him/herself in the same physical environment both on and off duty. On the battlefield, monitoring and surveillance is essential both for C2 and security; C2 systems are used to keep track of the location and movement of own and enemy units, to help the commander use his/her resources more optimally which will increase the level of security for all soldiers in the force. In case of emergency, the soldiers' lives may even depend on how well they are monitored, as in how fast you can be provided with reinforcements, medical support, or accurate intelligence information. Since this direct relationship exists between monitoring and survival, the troops generally accept it as they regard security as a need overtrumping that of privacy.

At the same time there are also other situations during military missions where privacy requirements are more plausible. This may be during off-duty hours in private quarters of the camp or in situations when performing personal hygiene. Furthermore, military resources may be the only ones available for communication, which can result in employees being reliant on the employer's resources for private correspondence. As ICT systems evolve, paying attention to possible ethical consequences becomes even more important (Stahl, Heersmink, Goujon, Flick, van den Hoven, Wakunuma, Ilkonen, and Rader, 2010). Adoption of emerging ICT, such as Software Defined Radio (SDR) and Mobile Ad hoc Network (MANET) systems, where the same equipment and infrastructure is used for many purposes, will even further emphasize the problem. In the military context, this can be represented by the same communications systems that are employed in a battle situation may also be utilized while off-duty back at base, used for personal communication with family and friends in the evening, or for private correspondence with lawyers or journalists. This fact raises questions of the emerging ethical implications of communications surveillance in these lines of work, where the importance of contextual integrity (CI) as described by Barth, Datta, Mitchell and Nissenbaum (2006) becomes apparent. CI focuses on explaining why some, seemingly identical, patterns of information flow can have different effects on privacy depending on whether the associated 'informational norms' are maintained or not. As an example, information that a soldier is HIV positive may be considered relevant information to a field surgeon before performing an operation, but may not be appropriate information to be spread among the general population of the mission.

Another recent research paper (Holbrook, 2010) compares privacy in the public workplace with that of the military workplace from a legal perspective, and reflects on the question of whether the unique realities of military service justify diminished privacy expectations in everything from garrison barracks to e-mail accounts. Although the law may give armed forces rights to carry out actions which limit the privacy of servicemen and women, such as non-consensual inspection of private living quarters and intrusive body cavity examinations, the ethical issues might be more complex. For instance, insecurity over privacy relating to medical information can have negative health impacts. Soldiers who have returned from military duty overseas may hide symptoms of post-traumatic stress disorder or depression, perhaps in fear of public disclosure or negative bias when seeking future commands, and consequently may not receive adequate treatment (Hébert, Flegel, Stanbrook and MacDonald, 2011; Zoroya, 2011).

Furthermore, it is relevant to question if the motivation for breaking privacy can vary between different military scenarios. As an example, consider a peace-time military exercise, and compare it to a disaster response scenario and finally a peace enforcement operation under war-like circumstances. These different scenarios may require different views on how the personal privacy of military personnel should be considered. In some cases breaking privacy, even though it may cause harm, might be the right choice, in others not. How can something that is ethically unjustifiable be acceptable in some cases and not in other cases? The natural response is that it depends on the circumstances and how you

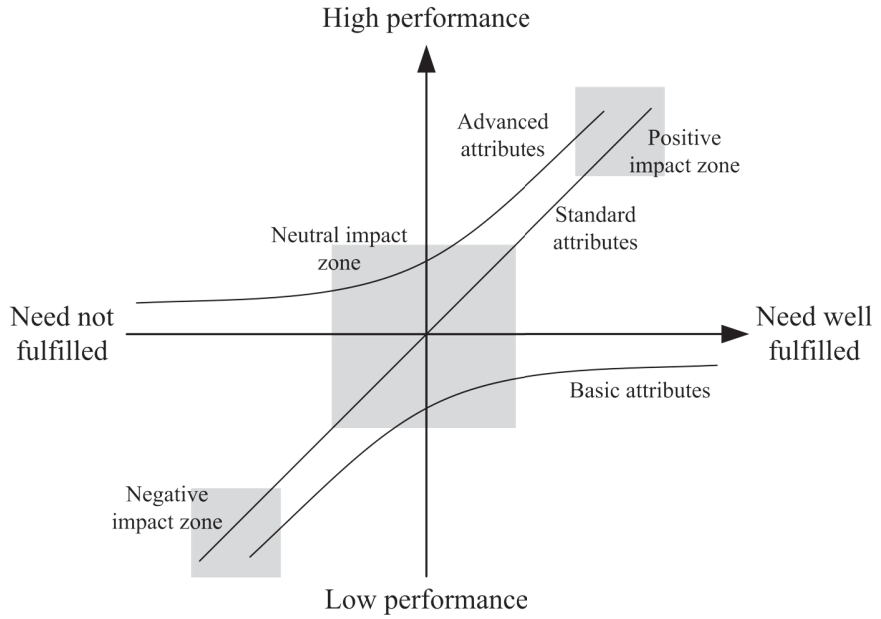

Figure 2. Kano model applied to soldier performance as a function of need fulfillment given by various attributes. Modified from (Kano, Seraku, Takahashi and Tsjui, 1984).

balance the consequences of the alternatives to the considered ethically questionable action. The rationale is thus based on utilitarian or consequentialist grounds, since the result would arguably be a greater good (or least harm). Equally, a greater wrong would be committed if the action would not to be carried out. This reasoning could also be supported by deontological reasoning, i.e. that morality is determined by actions not results. We cannot evaluate morality based on consequences or results because we do not know the full scope of those results, which are based on the sum of all future effect. We must thus base our moral decisions primarily on the actions themselves and not on the possible outcomes.

We do not have a general framework for determining when and why privacy intrusions are ethically justifiable. Based on a deontologist standpoint, each extreme situation would have to be analyzed on a case-by-case basis, in order to weigh the seriousness of the particular situation from different standpoints. In the case of privacy-affecting security technology, civilian applications (e.g. for public video surveillance) are commonly subject to scrutinization by regulatory agencies, as well as media and the general public, ensuring legal and ethical tenability. Security technology intended for military use (e.g. tactical communication surveillance), on the other hand, is usually not designed with privacy protection as the main objective. Although this is comprehensible during times of war or in emergency situations, the problem arises when security technology from the military domain is introduced in everyday society with the same stance towards privacy and identity protection, such as by government security or intelligence agencies in the name of national security or the war on terror.

SOLDIER PERFORMANCE

In order to determine what effects privacy, or the lack of privacy, may have on the battlefield we need a model that links privacy as a contextual attribute to how well the soldier functions in his or her environment. We have chosen to use the classic Kano model (Figure 2) as a basis, a theory originally developed to improve product development by reflecting customer satisfaction as a function of need-fulfillment (Kano, Seraku, Takahashi and Tsjui, 1984). To better suit our goals, the model has been

adapted to show how soldier performance, rather than satisfaction, is dependent on the fulfillment of various needs. The performance of the individual soldier in a given context (e.g. a war-like peace enforcement mission or a peace-time exercise) may thus be seen as a result of how well his or her needs are met, defined by various circumstance-related *attributes*. In the model, these attributes can be categorized as being *basic*, *standard* or *advanced*.

As previously established, soldier needs while performing his or her duties may vary greatly depending on the context. Furthermore, different attributes play separate roles in fulfilling these needs; some with a powerful relation to a certain need-fulfillment, others playing a smaller role. A *basic attribute* may be the availability of sufficient food rations or having other essential physical needs met. Basic attributes match needs that will not significantly contribute to increasing the soldier performance if met, but if these needs are not adequately fulfilled, the negative impact will be substantial. *Standard attributes* include efficient weaponry, transportation, intelligence and C2. These attributes may contribute positively as well as negatively to soldier performance, depending on how well they meet the needs. Since needs associated with these attributes are fairly well-known and predictable, the extent to which they are fulfilled is often a question of resource availability. *Advanced attributes* are those which, for the most parts, match needs which are unforeseen by the soldier. They may lie outside of normal routines or previous training, and thus do not contribute negatively to performance if the related needs are not met. However, if the needs are in fact met, the result may be a great increase of performance. In the original Kano model, the product attributes leading to fulfillment of advanced needs are those who help customers discover needs that they never thought about before. Analogously, advanced circumstance-related attributes are those that, if fulfilling a need, may result in exceptional soldier performance and thus provide a significant strategic advantage over the adversary.

The Kano model offers insight to the drivers behind soldier performance. A soldier may perform reasonably well by only relying on needs fulfilled by basic and some standard attributes. However, in order to achieve extraordinary results, the soldiers need to have needs met which they themselves may not be aware of, spurring creativity and promoting new use of available assets. Creativity, individual initiatives and freedom of action are the foundation of the Mission Command doctrine (also known by its German name: *Auftragstaktik*), employed by many armed forces around the world, promoting a decentralized military command style. As combat situations are commonly characterized by being complex and dynamic, soldiers are forced to act while maintaining a high tempo, basing decisions on incomplete or low-quality information. Unforeseen problems must be handled quickly, using the resources at hand. Simultaneously, sudden valuable opportunities, which may lead to high-effect results, must be taken and adequately exploited. This leads us to theorize that well-designed C2 systems could provide a great advantage to the units, acting as an *advanced attribute*. However, privacy is to be regarded a *basic attribute* as it does not render significant advantages in combat but it could potentially reduce the troops' creativity if not fulfilled in the same manner as Kizza and Ssanyu reported for office workers (2005) and Miller for police (2005). An ICT that increases C2 capability but infringes privacy to the level where a soldier feels discomfort is not guaranteed to have a positive effect on performance; in fact it may even be negative (Kizza and Ssanyu, 2005) depending on how the soldier reacts to the violated privacy.

SOME EMERGING MILITARY ICTS

When evaluating the adoption of a certain security technology one needs to be aware of the full consequences of using that technology, not only for the organization but also for the individual users and possibly also in a larger perspective for society as a whole. The consequences of not using the same technology should also be investigated, and used as a reference for comparison. Security technology for military use is often designed for the situation which requires the most of the system, predominantly a situation of conflict or war. This has several implications when the same system is used in another context. An invasion of privacy that might be acceptable in a war-time scenario might be ethically questionable during a peace-time exercise.

Blue Force Tracking (BFT) is a military technology used to track location of friendly units (Lawler, 2003; Conatser and St. Claire, 2003). Ultimately this technology allows for tracking each and every soldier in the friendly forces to prevent accidental friendly fire. The technology was designed for war-like conditions and is not as likely to be used in peace-time scenarios. However, even in war, soldiers have time to go off-duty and recover. A question then arises; shall the troops still be tracked with the BFT system for their own safety while going off-base during their rest and recreation phase, regardless if the leave is sanctioned or not? An example of such an incident is the case of the U.S. Army soldier Ahmed Kousay al Taie who was kidnapped while sneaking off base in Iraq in 2006 and still remains MIA (Gamel, 2011). While it is not clear that a BFT system would have been able to help this particular soldier, there is at least a possibility. However, if such a system would have been available to soldiers in a similar scenario, it is still quite unlikely, for obvious reasons, that they would want to make use it while sneaking off base.

A second example is the *Joint Tactical Radio System* (JTRS), which is being put forward as the future tactical communications platform for all of the U.S. armed forces. Many other countries, including Sweden, are developing their own versions of this system in close collaboration with the United States. JTRS seeks to benefit from Software Defined Radio (SDR) technologies to implement a tactical IP-based mobile ad hoc network (MANET) as a platform which should fulfill all future military communication needs (Sigholm, 2010). All types of communication, ranging from the sending of tactical messages between units on the battlefield to private web surfing during a peace-time exercise, are supported by the system. In these MANET-based networks, data is transmitted from one node to another, by letting other nodes on the path between the sender and receiver relay the message one hop at a time. This allows for creating large networks which need not rely on any fixed infrastructure, such as cell towers in mobile telephony systems.

However, there are several challenges with this type of network setup which may lead to ethical pitfalls. For instance, the task of selecting the optimal path for information flow is more difficult and requires knowledge about unit locations. As in the example of BFT above, this may lead to detailed tracking of soldiers carrying this equipment. Another potential ethical problem is that the system requires better defense against node compromization, meaning adversary control over the radio unit either physically or by use of some malware (e.g. computer virus or Trojan horse software). To protect against this, special surveillance code can be placed in the units to guard against irregular communication. This may at first glance seem like a legitimate cause, but if all communication is monitored, albeit for security purposes, there is still a risk of valid correspondence incorrectly being flagged as anomalous, and subsequently being intercepted and surveyed. This risk was also one of the main concerns in the discussions surrounding the Swedish FRA signals intelligence law and the implementation of the anti-piracy IPRED EU directive mentioned earlier. As seen in polls, most people would agree to communication surveillance aimed at exposing terrorist schemes, while the prospect of having one's own lawful correspondence checked by mistake is a commonly a source of unease for a majority of the population. It would probably also hold true in a comparable military scenario.

Yet another example is the use of *head-mounted cameras* to provide live feeds to reach-back centers. An example is the raid on Osama bin Laden (Harden, 2011) that was allegedly being watched in real-time by the White House in Washington D.C., albeit with some technical issues according to CIA (Swinford, 2011). Using such video feeds means that anyone watching is directly able to judge and question every move made. This is an extreme case of workplace monitoring, that no doubt will cause an infringement of privacy, but the question is to what level it affects the troops. It is reasonable to believe, although not certain, that during said raid the soldiers did not think much of the cameras as they were preoccupied with their mission. However, any mistake they made would be broadcasted directly to the highest authority. The mere awareness of that broadcast could possibly have affected soldiers as the mission went on, or even caused anxiety among soldiers afterwards, not knowing whether their mistakes and mishaps were being observed by the president or not.

Data minimization	Variable amount of collected data and variable storage times
Transparency	The clients (users) are aware of when they are being monitored
Personal data safeguards	Protection of user data that is being stored or transferred
Anonymity	Variable level of detail, i.e. the possibility to group users
Pseudonymity	Possibility to replace actual user name with an alias
Access control	Access to personal data only on a need-to-know basis

Table 1. A collection of Privacy Enhancing Technologies relevant to the privacy of battlefield communication and C2 systems.

PRIVACY ENHANCING TECHNOLOGIES

Privacy Enhancing Technologies (PETs) are technical solutions which contribute to maintaining or enhancing privacy in systems managing personal information, such as security ICT systems, with the goal of not limiting the systems' functionality or efficiency (Raguse, Langfeldt and Hansen, 2008). PETs achieve this by minimizing the amount of privacy-related information stored in the system, and by preventing or limiting access to this information. An overview of suggested PETs which could be relevant for future military communications and C2 systems is shown in Table 1 above. These technologies are not mutually exclusive, but each come with pros and cons that make them more or less usable in different military scenarios. Each will be described in detail below where we will use the term subject to denominate the soldiers exposed to privacy infringement by the system, e.g. the soldiers on the battlefield. We also refer to the examples given above as to when each PET might be especially appropriate or applicable.

Data minimization is the principle of making sure that only data that is absolutely needed is also collected, and that it is discarded when no longer needed. This PET is designed to minimize the time and extent of the exposure, but not remove it. While limiting the extent is certainly positive, it is not certain that shortening the time is actually helping since the subjects may feel violated immediately just by knowing that they are exposed. In regard to localization technologies, a data minimization PET can be applied to limit storage times of position data and the level of detail stored. When sending live video feeds the PET could be used to ensure that streaming is only enabled when deemed appropriate.

The idea of *transparency* is to make the subjects always know when they are being exposed to the possible privacy infringement. The purpose is to develop trust so that the subjects do not have to feel insecure when they are not monitored. The main drawback is that by knowing they are exposed they may already feel exposed and as a result performance drops, just as Kizza and Ssanyu reported (2005). In the cases of technology which locates individual soldier, such as BFT systems or location-based routing JTRS units, transparency mechanisms allow the soldier to know when he or she is being located or tracked, or when communication is being monitored. Without mechanisms for transparency, the soldier immediately loses all control over personal data being collected, and therefore also loses his or her privacy according to the definition of Aiello & Knob (1996).

Several mechanisms can be used to create *personal data safeguards*. These are required to protect personal data at rest, or in motion, against compromise by upholding the basic computer security properties confidentiality, integrity and availability. The safeguards should also guarantee that, if transparency cannot be maintained, subjects are made aware in retrospect who accessed their data, what parts of it that was read and for what purposes. This ensures later control by the user and helps facilitate legitimate use of the security technology. In the case of monitoring of JTRS communication, personal data safeguards should be put in place to ensure that data is protected to the full extent of available technology. If legal interception of communication is performed, the user should be informed of this after the investigation has ended.

The concept of *anonymity* is that of removing any information that can tie the data to a specific individual. Anonymity is useful when for instance group behavior is studied and the actual identities

behind data do not matter. In scenarios where identity does matter, anonymity is not applicable. However, in scenarios with massive data collection it can be hard to guarantee anonymity as multiple anonymous data sets can be used to render profiles which in turn can re-identify subjects, which has been shown by e.g. Benoist (2008). When BFT systems are used anonymity PET could be employed to vary the resolution of the unit being tracked depending on the need and context. In some cases it might for instance only be necessary to track units on platoon or company levels, and not down to the individual soldier.

Pseudonymity is related to anonymity in the sense that the idea is to de-identify persons. With pseudonymity however, the link is still kept to the original subject through use of a unique identifier. This solves the problem of anonymity in scenarios grouping data from one source is vital for it to make sense, but the actual identity of the subject is not important. It does so however, at the cost of a higher risk for re-identification as it simplifies the profiling process mentioned above. Pseudonymity can be a very useful PET, especially in combination with access control described below. By removing the identity of the subject which is being surveyed, and allowing only people with special clearance or in certain roles to authorize a re-identification, appropriate privacy levels may be upheld while still allowing for precise identification in cases where it is absolutely needed. Transparency may also give the subject knowledge of the current level of pseudonymity.

Access control is probably the most commonly used PET as it is easy to implement in controlled environments. The concept is that data may be extensively captured and stored, but only viewed by authorized people and only when it is needed. The main problem with access control is that 'when needed' is subjective. The subjects may not agree to the reasons for being under surveillance, or even be aware of that their data is being accessed. This can cause a sensation of unrest, even if the data is in fact never actually examined. Access control is an important PET and may be used in all examples above. It is also important in order to uphold the personal data safeguards.

It should be noted that none of the PETs mentioned above are absolute in the sense that their existence means they always have to be employed. There is nothing that contradicts the systems to implement several of these technologies, allowing them to be configured specifically for the purpose they are being used at a specific time. However, the 'human factor' must not be neglected and the subjects may therefore have issues trusting a system with the potential to infringe on their privacy if not properly configured.

DISCUSSION

In this paper we have studied the concept of battlefield privacy and how emerging military ICTs may come to affect the conditions for the professionals tasked with protecting our society from various threats. During our work we have discovered that the area of military privacy contains very limited amounts of previous research. We have thus made use of established privacy research within the civilian society as a baseline. There we have seen that the issue of privacy can not only at times be politically sensitive, but that it may also vary substantially depending on the context. It appears that when we feel threatened, privacy seems less important to us than when we feel secure. The need for privacy also seems to be something highly individual; where some treasure their privacy greatly, others seem not to care as much.

We have further established that excessive privacy invasion, such as workplace surveillance, may have a severe negative impact on the self-esteem, creativity and performance of employees. Depending on the situation, privacy-infringing surveillance may also be morally unjustified according to basic ethical principles. This leads us to presume that privacy issues may also be relevant in the 'military workplace', which has increasingly come to rely on the use of potentially privacy-infringing ICTs. These systems are designed to increase troop performance, but could it instead be the case that lack of privacy could actually decrease the soldiers' performance in some situations?

In order to enable theorizing, and to give some preliminary insight as to how privacy affects warfighter performance, we have provided a novel model which illustrates performance as a function of need fulfillment given by various attributes. The model has not yet been verified empirically, but we believe it will be a good reference point for future theories on the effects of military ICTs. We regard privacy as a basic attribute, but it is important to stress that results should be considered for a specific, given context.

We have pointed out the option of implementing PETs in emerging ICT-dependent systems, in order to reinforce and strengthen privacy on the battlefield, to avoid or mitigate the effects of the anticipated ethical pitfalls, and to shift emphasis of missions from being control-oriented into being more characterized by consistency between rules and culture. We have also tried to pinpoint a few different scenarios where emerging ICT technology put the soldier in risk of being exposed to privacy infringement. We argue that military technology developers should start thinking in terms of PETs to limit the negative consequences of the new technology, since even if the negative impact on performance cannot be proven, there may still be an ethical issue as the privacy infringement may also cause anxiety among solders long after the actual incident.

Another relevant question to ask is if infringing soldiers' privacy is perhaps justifiable. There is surely a valid argument in that soldiers will face much worse circumstances in combat, which may also cause anxiety and post-traumatic stress disorder later on. We believe the answer to this question of justifiability lies in investigating the options. If the only other alternative is to not have these technologies and expose the soldiers to a greater risk of getting killed, then there is no doubt that privacy is a small price to pay for security. However, if PETs can reduce the privacy infringement while keeping the safety capability, then can we morally defend not to use them? As so often in ethics, it becomes a tradeoff, in this case to find the perfect balance between security and privacy.

This study does not present any data showing evidence of privacy violations causing performance limitations on the battlefield. Yet, backed with results from privacy research within the civilian sector, we allow ourselves to define two hypotheses: (1) extensive use of emerging military ICTs gathering personal data, without proper PETs employment, will lead to soldiers' privacy being violated, and (2) these violations will result in an observable performance drop. We now call upon the research community to verify or reject these two hypotheses. In the meantime, we urge defense procurement agencies to keep privacy aspects in mind when acquiring ICTs for their troops. We believe that neglecting the privacy perspective, while ICT continues to evolve unrestricted for troop command and control, could result in consequences which are not easy to grasp in advance.

REFERENCES

Aiello, J. R. and Knob, K. J. (1996) Electronic Performance Monitoring: A Risk Factor for Workplace Monitoring. In: S. L. Sauter and L. R. Murphy, eds. *Organizational Risk Factors and Job Stress*, Washington, DC: American Psychology Association, pp.163-179.

Allan, A. and Warden, P. (2011) Got an iPhone or 3G iPad? Apple is Recording Your Moves – A Hidden File in iOS 4 is Regularly Recording the Position of Devices. *O'Reilly*, [online] (Updated Apr. 27, 2011), available at: <http://radar.oreilly.com/2011/04/apple-location-tracking.html>, retrieved May 12, 2011.

Bajoria, J. (2010) The Debate Over Airport Security. *Council on Foreign Relations*, [online], available at: <http://www.cfr.org/air-transportation-security/debate-over-airport-security/p23673>, retrieved May 10, 2011.

Ball, H. (2004) The U.S.A. Patriot Act of 2001: Balancing Civil Liberties and National Security. Santa Barbara, CA: ABC-Clio Inc.

Barth, A., Datta, A., Mitchell, J. C. and Nissenbaum, H. (2006) Privacy and Contextual Integrity: Framework and Applications. *27th IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, May 21-24, 2006.

Benoist, E. (2008) Collecting Data for the Profiling of Web Users. In: M. Hildebrandt and S. Gutwirth, eds. *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Netherlands.

Bigo, D., Shapiro, J. and Fedorov, A. (2004) European Homeland Security Post-March 11th and Transatlantic Relations. In: F. Heisbourg, ed. *European Security Forum, Working Paper No. 17*, Oct. 2004.

Conatser, J. and St. Claire, T. (2003) Blue Force Tracking – Combat Proven. *Armor Magazine*, **112**(5), Sep. 2003, pp.20-23.

Deibert, R., Palfrey, J., Rafal, R. and Zittrain, J. eds. (2010) Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace. Cambridge, MA: Massachusetts Institute of Technology Press.

Eriksson, M. (2011) Android Location Service Cache Dumper. *GitHub Inc.*, [online] (Updated Apr. 21, 2011), available at: <https://github.com/packetlss/android-locdump>, retrieved May 11, 2011.

European Commission (2011) Data retention: Commission refers Sweden back to Court for failing to transpose EU legislation. [press release], Apr. 6, 2011, available at: <http://europa.eu/rapid/press ReleasesAction.do?reference=IP/11/409>, retrieved May 11, 2011.

European Parliament (2006) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. *Europa.eu*, Available at: <http://www.dataretention2010.net/files /legislation/dataretention/Directive_2006_24_EC_EN.pdf>, retrieved May 11, 2011.

Fried, I. (2011) Google: Of Course our Location-based Services Require Your Location Info. *Mobilized*, Apr. 22, 2011, available at: <http://mobilized.allthingsd.com/20110422/google-of-course-our-location-based-services-require-your-location-info>, retrieved May 12, 2011.

Gamel, K. (2011) Search Goes on for Missing Americans in Iraq. *The Associated Press*, Jan 21, 2011, available at: <http://www.armytimes.com/news/2011/01/ap-search-goes-on-for-missing-americans-in-iraq-012111/>, retrieved May 12, 2011.

Granick, J. (2006) Security vs. Privacy: The Rematch. *Wired magazine*, May 24, 2006, available at: <http://www.wired.com/politics/law/commentary/circuitcourt/2006/05/70971>, retrieved May 11, 2011.

Harden, T. (2011) Osama bin Laden killed in Pakistan. *The Telegraph*, May 2, 2011.

Hébert, P. C., Flegel, K., Stanbrook, M. B and MacDonald, N. (2011) No privacy of health information in Canada's Armed Forces. *Canadian Medical Association Journal*, **183**(3), Feb 2011, pp.167-168.

Holbrook, J. (2010) Communications Privacy in the Military. *Berkeley Technology Law Journal*, **25**(2), pp.831-908.

Howard, C. (2010) Achieving the information advantage. *Military & Aerospace Electronics magazine*. **21**(7), Jul. 2010.

Jamieson, A. (2010) Suspected suicide bomb in central Stockholm injures two and panics shoppers. *The Telegraph*, Dec. 11, 2010.

Kano, N., Seraku, N., Takahashi, F. and Tsjui, S. (1984) Attractive quality and must-be quality. *Hinshitsu*, vol. 14, no 2, pp.147-156.

Kizza, J. M. and Ssanyu, J. (2005) Workplace Surveillance. In: J. Weckert, ed. *Electronic Monitoring in the Workplace: Controversies and Solutions*, Hershey, PA: Idea Group Inc. Publishers.

Kravets, D. (2009) Pirate Party Wins EU Parliament Seat. *Wired Magazine blog*, [blog] Jun. 8, 2009, available at: <http://www.wired.com/threatlevel/2009/06/pirate-party-wins-eu-parliament-seat/>, retrieved May 11, 2011.

Lawlor, M. (2003) Keeping Track of the Blue Forces. *Signal Intelligence Journal*, Armed Forces Communications and Electronics Association (AFCEA), **57**(11), pp.37-39, Jul. 2003.

Left, S. and Oliver, M. (2005) 38 dead in London blasts. *The Guardian*, Jul. 7, 2005.

Malek, J. (2005) Informed Consent. In: C. Mitcham, ed. *Encyclopedia of Science, Technology and Ethics*, vol. 2, Detroit: MacMillan Reference USA, pp.1016-1019.

Miller, S. (2005) Guarding the Guards: The Right to Privacy, and Workplace Surveillance and Monitoring in Policing, In: J. Weckert, ed. *Electronic Monitoring in the Workplace: Controversies and Solutions*, Hershey, PA: Idea Group Inc. Publishers.

Nissenbaum, H. (2005) Where Computer Security Meets National Security. *Ethics and Information Technology*, **7**(2) pp.61-73.

Pernemalm, P. and Lindgren, M. (2011) Ungdomar och integritet (Youth and integrity). *The Swedish Data Inspection Board Report 2011:1*, Stockholm: Kairos Future.

Patriot Act (2001) Public Law 107 - 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, available at: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56>, retrieved May 10, 2011.

Raguse, M., Langfeldt, O. and Hansen, M. (2008) Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies, *European Commission Seventh Framework Programme, project PRISE. Deliverable 3.3 Proposal Report*.

Richburg, K. B. (2004) Madrid Train Blasts Kill at Least 190. *The Washington Post*, Mar. 12, 2004.

Ricknäs, M. (2011) Swedish Parliament Delays Approval of Data Retention Law. *PC World*, Mar. 17, 2011, available at: <http://www.pcworld.com/businesscenter/article/222426/swedish_parliament_delays_approval_of_data_retention_law.html>, retrieved May 11, 2011.

Rotenberg, M. (2007) Privacy vs. Security? Privacy. *The Huffington Post*, Nov. 9, 2007, available at: <http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-priva_b_71806.html>, retrieved May 10, 2011.

Sandels, A., Stobart, J. (2010) Denmark Terrorism Plot Thwarted with Arrest of Five Suspected Militants, Authorities Say. *Los Angeles Times*, Dec. 30, 2010.

Schneier, B. (2008) What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites. *Wired.com*, available at: <http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124>, retrieved May 11, 2011.

Sigholm, J. (2010) Reconfigurable Radio Systems: Towards Secure Collaboration for Peace Support and Public Safety. *9th European Conference on Information Warfare and Security (ECIW 2010)*, Thessaloniki, Greece, Jul. 1-2, 2010.

Stahl, B. C., Heersmink, R., Goujon, P., Flick, C., van den Hoven, J., Wakunuma, K. J., Ilkonen, V. and Rader, M. (2010) Issues, Concepts and Methods Relating to the Identification of the Ethics of Emerging ICTs. *Communications of the IIMA*, **10**(1), pp.33-43.

Swinford, S. (2011) Osama bin Laden Dead: Blackout During Raid on bin Laden Compound. *The Telegraph*, May 4, 2011.

Tavani, H. T. (2008) Informational Privacy: Concepts, Theories, and Controversies, In: K.E. Himma and H.T. Tavani, eds. *The Handbook of Information and Computer Ethics*. New Jersey: Wiley & Sons.

Warren, S. D. and Brandeis, L. D. (1890) The Right to Privacy. *Harvard Law Review*, vol. 4, no. 5.

Wright, L. (2008) The Spymaster: Can Mike McConnell Fix America's Intelligence Community? *The New Yorker*, [online] available at: <http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright>, retrieved May 11, 2011.

Woo, M. (2008) Wanted: Tactical Radio Strategy. *Military Information Technology Magazine*, **12**(8), Sep. 2008.

Zoroya, G. (2011) Army suicide prevention efforts raising privacy concerns. *USA Today*, [online], available at: <http://www.usatoday.com/news/military/2011-03-31-army-suicide-prevention-privacy_N.htm>, retrieved: May 11, 2011.

BIOGRAPHY

Capt. Johan Sigholm is a Ph.D. student in Military Technology at the Swedish National Defence College in Stockholm, Sweden, and the National Defence University in Helsinki, Finland. He is an officer in the Swedish Air Force and received his M.Sc. degree in Computer Science and Engineering from Linköping University, Sweden. His research is currently focused on studying how emerging ICT can be used to support and facilitate work for military personnel engaging in inter-organizational collaboration.

Mr. Dennis Andersson holds an M.Sc. in Computer Science at Linköping University, where he is now enrolled as a Ph.D. student in the area of Informatics. He is employed at the division of Information Systems at the Swedish Defence Research Agency where his main focus is on evaluating complex military and crisis management training. At the time of writing this paper, his main affiliation is the Naval Postgraduate School in Monterey, CA, where he is working on Case-based reasoning models for distributed experimentation in maritime operations.