Salient but Unappreciated: Issues in National and International Security and Defense Policy for the Next Decade

Christian Geib

The author would like the following persons: Thomas Schafbuch and the whole editorial team on the Journal on Terrorism and Security Analysis for their tireless support and patient editing, my fellow LL.M. student Moran Druker at Stanford Law School for her suggestions and research concerning the "Iron Dome" and Professor Drury Stevenson of the University of South Texas College of Law for directing my attention to the "Black Swan" and insurance considerations through his intriguing presentation at the Defense Policy Symposium at Stanford on Jan. 22, 2011 and his inspiring article, The Effect of National Security on the Criminal Law Paradigm.

1. The Neglected Issues of Combined Arms -the Hubris of Predicting Future Warfare:

As much as scholars of all academic disciplines would like to think of their discipline as purely based on observation and analysis, undoubtedly they are subject to temporary fashion cycles which influence the debate beyond mere scientific findings and scientific reasoning.

Military strategy and defense policy are no exception to that. Throughout military history, military thinkers have been subject to such cycles with concerns to the question of what really was at the contemporary *cutting edge* nature of warfare and what the future of warfare would be like.

As most prominently articulated in the "Rumsfeld Doctrine[1]" with its emphasis on ever lighter, Special Forces-focused *Blitzkrieg* approach, currently to most defense policy planners and scholars it appears that *counterinsurgency*[2] (COIN) or *counterterrorism* are "the only games in town" for future military campaigns. Large Cold War-like ground forces are synonyms for being *obsolete* in modern defense policy and portrayed as being, once and for all, a phenomenon of the past.

Instead, the future seems to be entirely dominated by *asymmetric warfare*, i.e. warfare with severe imbalances of strength between the combating parties.[3] Part of this apparently inevitable asymmetrical future combat scenario is to be the so called *"Three Block Warfare."*[4] The concept of the "three-block war" was promulgated by Marine Corps General Charles Krulak.[5] Krulak realized that on the modern battlefield, Marines could be called upon to perform very different missions simultaneously. On one block they might be engaged in high-intensity combat, on the next block they might be handing out relief supplies and on the third block they might be separating warring factions.[6]

Small, light, modern, highly expeditionary forces for swift peacekeeping, peace enforcement, evacuation, counterterrorism or counterinsurgency missions appear to be the military strategy consensus amongst most major European NATO powers, such as England, France and Germany, who have recently agreed on substantial cuts and restructuring of their military in sheer numbers and "heavy" equipment.[7]

---

[1] Carl Robichaud, *Failings of the Rumsfeld doctrine-Intense air power and small groups of troops didn't win in Iraq or Afghanistan (*September 21, 2006), http://www.csmonitor.com/2006/0921/p09s02-coop.html (last visited Dec. 31, 2010); Michael E. O'Hanlon, *A Reality Check for the Rumsfeld Doctrine*, (APRIL 29, 2003); http://www.brookings.edu/opinions/2003/0429defense_ohanlon.aspx , (last visited Dec. 31, 2010).

[2] Especially following the widely acclaimed work of one of the leading scholars in this field, David Kilcullen and his most recent publications: DAVID KILCULLEN, THE ACCIDENTAL GUERRILLA: FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE (2006); DAVID KILCULLEN, COUNTERINSURGENCY (2010).

[3] Id. At 22: "In mid-2008 supplemental budget allocation for the Iraq war the , the US defense budget is approaching 70 percent of the global defense spending which is bound to make any military engagement of the United States against another party highly asymmetrical; Richard Norton-Taylor, *Asymmetric warfare Military planners are only beginning to grasp the implications of September 11 for future deterrence strategy,* THE GUARDIAN, (from October 3, 2001), http://www.guardian.co.uk/world/2001/oct/03/afghanistan.socialsciences (last visited Feb. 7, 2011); Toni Pfanner, *Asymmetrical Warfare from the Perspective of Humanitarian Law and Humanitarian Action,* Vol. 87 No. 857 (March 2005), https://docs.google.com/viewer?url=http://www.icrc.org/eng/assets/files/other/irrc_857_pfanner.pdf (last visited on Feb. 7, 2011): "The fundamental aim of asymmetrical warfare is to find a way round the adversary's military strength by discovering and exploiting, in the extreme, its weaknesses. Weaker parties have realized that, particularly in modern societies, to strike "soft targets" causes the greatest damage. Consequently, civilian targets frequently replace military ones... The term "symmetrical warfare" is generally understood to mean classic armed conflict between States of roughly equal military strength.7 The wars that took place in the eighteenth and nineteenth centuries — i.e. after the Peace of Westphalia — in which evenly matched government troops confronted and fought each other in open battles have sometimes been called a thing of the past, for in the twentieth century wars became more complex and more unequal. Furthermore, most wars nowadays are internal, although they frequently have international ramifications. They are as diverse as they are numerous and the way in which they are conducted varies according to the type of conflict…" (at 151-52).

[4] Also referred to as Fourth-Generation Warfare, see: Tony Corn, *World War IV was Fourth-Generation Warfare,* HOOVER INSTITUTION STANFORD UNIVERSITY POLICY REVIEW JAN. 2006, http://www.hoover.org/publications/policy-review/article/6526 (last visited Feb. 8, 2011).

[5] Max Boot & Jeane J. Kirkpatrick, *Beyond the 3-block war*, ARMED FORCES JOURNAL in: Council of Foreign Relations (March 2006), http://www.cfr.org/united-states/beyond-3-block-war/p10204?breadcrumb=/publication/publication_list%3Ftype%3Djournal_article%26page%3D10 (last visited Feb. 7, 2011).

[6] Id.

[7] *Germany's Responsible Military Reform,* The New York Times, December 29, 2010, at A 28; *Military Reform: Conscription in*

However, when such theories like the "Rumsfeld Doctrine" were put to the test during operation *Iraqi Freedom* in 2003, the lack of sufficient "boots on the ground" in itself posed a problem with stabilizing Iraq immediately after major combat operations had ended in 2003.

Already during the initial "shock and awe" phase of the 2003 Iraq campaign it became apparent that the great strength of the "outdated" old, heavy armor lay in its great robustness. On a number of occasions, even in situations of being heavily outnumbered, during operation *Iraqi Freedom* the M1 Abrams tanks stood their ground in situations where lighter and more *modern* Striker Brigades would have suffered substantial numbers of casualties.[8]

German troops in Afghanistan had shown that unexpectedly it was not the swiftly moving "modern" light infantry that dominated the fierce fighting in their sector, but the old-fashioned, Cold War-like, slow moving armored infantry, the *Panzergrenadiers*.[9] This was illustrated by a number of fierce firefights with insurgents in the Northern Province of Kunduz.

In one firefight a platoon of German Army paratroopers was ambushed during a foot patrol on April 2, 2010 in the village of Isa Khel.[10] During this firefight the German platoon was outgunned and outnumbered. The German paratroopers and the supporting armored vehicles were only equipped with assault rifles of 5.56 mm caliber and machine guns of 7.62 mm caliber. The insurgents made use of strategically positioned improvised explosive devices (IED) (which destroyed one of the vehicles trying to evacuate some of the wounded soldiers), AK-47 assault rifles, heavy machine guns, rocket propelled grenades (RPG) and mortars. Due to the vicinity of populated areas and scarcity of combat helicopters in this Province of Afghanistan, air support (other than for mere show of force) could not be

---

Germany to End Next Summer, DER SPIEGEL, Nov 23, 2010, http://www.spiegel.de/international/germany/0,1518,730660,00.html (last visited Dec. 31,2010); *In Retreat German Military Reform Could Halve Ground Forces,* DER SPIEGEL, Aug. 9,2010, http://www.spiegel.de/international/germany/0,1518,710853,00.html, (last visited Dec. 31, 2010); Robin Bravender, *European countries downsize military, increase social programs,* (October 30, 2006), http://www.theeagleonline.com/news/story/european-countries-downsize-military-increase-social-programs/ (last visited Dec. 31, 2010); *SAS cuts raise concerns over UK's military strength,* (September 16, 2010), http://rt.com/news/sas-downsize-budget-slash/; (last visited Dec. 31, 2010); James Kirkup, *Defense spending: thousands of troops to be cut* (Sep 10, 2010), http://www.telegraph.co.uk/news/newstopics/politics/defence/7995646/Defence-spending-thousands-of-troops-to-be-cut.html (last visited Dec. 31, 2010); DAVID STRINGER, *British Armed Forces Cuts Announced: UK Addresses Deficit, Trims Defense Spending* (Oct. 19,2010), http://www.huffingtonpost.com/2010/10/20/royal-armed-forces-cuts-a_n_769446.html, (last visited Dec. 31, 2010); *U.K. Defense Spending Cuts Worry Clinton*, CBS News (Oct. 15, 2010), http://www.cbsnews.com/stories/2010/10/15/world/main6960705.shtml (last visited Dec. 31, 2010); Henry Chu Los Angeles Times, *European allies to slash military spending While officials point to big budget deficits, critics say they will cede their role on the world stage* (Dec. 26, 2010), http://www.philly.com/inquirer/world_us/20101226_European_allies_to_slash_military_spending.html (last visited Dec. 31, 2010); Pierre Tran , *France To Cut Spending $4.8B Over 3 Years* (Sep 28, 2010), http://www.defensenews.com/story.php?i=4799913 (last visited Dec. 31, 2010*); Germany - Military Spending,* GlobalSecurity.Org, (July 2010), http://www.globalsecurity.org/military/world/europe/de-budget.htm (last visited Dec 31, 2010); Spencer Ackerman, *Deficit Plan Scraps Pentagon Jets, Tanks, Trucks*, (November 10, 2010), http://www.wired.com/dangerroom/2010/11/deficit-plan-scraps-pentagon-jets-tanks-trucks/ (last visited Dec. 31, 2010); Hans Binnendijk et. al, *Defense Cuts: A Rescue Plan for NATO* (November 4, 2010), http://www.atlantic-community.org/index/articles/view/Defense_Cuts:_A_Rescue_Plan_for_NATO_ (last visited December 31, 2010); *Budget Cuts Are a Good Pretext for Reforming Military Policy*, DEFENCE TALK (SEPTEMBER 8, 2010), http://www.defencetalk.com/budget-cuts-are-a-good-pretext-for-reforming-military-policy-28597/ (last visited December 31, 2010).; Quentin Peel and James Blitz, *Security: A German military overhaul,* FINANCIAL TIMES FT.COM (Published: January 31 2011 09:07 pm Last updated: January 31 2011 09:07 pm), http://www.ft.com/cms/s/0/c0fedfdc-2d6f-11e0-8f53-00144feab49a.html#axzz1DYuBNyBv (last visited Feb.9, 2010); *New model army,* FINANCIAL TIMES FT.COM, Published: November 18, 2010 10:55 pm, Last updated: November 18, 2010 10:55pm) http://www.ft.com/cms/s/0/9253fe06-f35e-11df-b34f-00144feab49a.html#axzz1DYuBNyBv (last visited Feb. 9, 2011):

> …Modernization was overdue. During the cold war, the German army's role was to act as a speed-bump for Soviet tanks dashing westwards. Times and threats have changed. But Germany maintains its static defensive posture. Although its army is one of the largest in Europe, its ability to deploy forces overseas is minimal… A professional army with greater expeditionary capacity will allow Germany to shoulder a greater burden in international operations. With pan-European defense cuts making inroads into the capacity of organizations such as NATO, this would be a positive development…

> During the Cold War, the German army's role was to act as a speed-bump for Soviet tanks dashing westwards. Times and threats have changed. But Germany maintains its static defensive posture. Although its army is one of the largest in Europe, its ability to deploy forces overseas is minimal…
>
> A professional army with greater expeditionary capacity will allow Germany to shoulder a greater burden in international operations. With pan-European defense cuts making inroads into the capacity of organizations such as NATO, this would be a positive development…

[8] David Talbot, *How Technology Failed in Iraq* (NOVEMBER 2004), http://www.technologyreview.com/computing/13893/ (last visited Dec. 31, 2010); Frank Lewis, *Iraq War veteran speaks about experiences in Baghdad*, (Nov. 1, 2010), http://www.portsmouth-dailytimes.com/view/full_story/9942416/article-Iraq-War-veteran-speaks-about-experiences-in-Baghdad?instance=home_news_lead (last visited Dec. 31, 2010);

[9] *Schützenpanzer Marder: Das 20-Millimeter-Argument*, German Army Homepage (July 16, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W287EAH5365INFODE/content.jsp (last visited Dec 31, 2010).

[10] Id.

deployed. Therefore, it took the German platoon and the reinforcements a several hour-long firefight to pull out of the area. During the firefight it became apparent that the 5.56 mm and 7.62 mm bullets of the German soldiers were not able to penetrate the thick clay walls of the surrounding buildings. Thus, the German paratroopers were not able to eliminate many emplacements of the insurgents. However, in return the insurgents with their RPGs *were* able to target German soldiers seeking cover behind the very same clay walls. In total 3 German soldiers were killed and 8 wounded.[11]

Moreover, a poorly marked vehicle of the Afghan National Army (ANA) that was rushing to the help of the German forces was targeted by German reinforcement troops as it approached them with high velocity. During this "friendly fire" incident 5 ANA soldiers were killed.[12]

Following this fierce firefight the German Minister of Defense zu Guttenberg ordered that the number of the available heavily armored infantry combat vehicle *Marder* for the German contingent be doubled. The *Marder* 1 A3 vehicle had originally been introduced into the German Armed Forces in the 1970s and developed for Cold War scenarios of large tank and infantry battles. With the end of the Cold War most military strategists viewed the *Marder* and the whole concept of heavily armored infantry as obsolete and inapt to adapt to modern challenges.[13]

However, this seemingly "obsolete" 38 metric ton *Cold War* vehicle with its 20mm canon soon proved its usefulness in the Northern Afghan Provinces once the German Army had taken over the responsibility of the *Quick Reaction Force* in the Northern ISAF sector.[14]

The *Marder* especially showed its usefulness during the fierce engagement at July 19, 2009 at Zar-Kharid-i-Sufla nearby Kunduz[15]:

A German *Panzergrenadier*-Platoon managed to rescue a unit of the Afghan National Army (ANA) that was accompanied by Belgian military advisers and had come under heavy fire from insurgents. The 20mm canon managed to eliminate insurgent emplacements behind thick stone and clay walls which rapidly ended insurgent resistance during this firefight.[16]

This constituted the kind of firepower and armor that was sorely missed during the engagement at Isa Khel.

As a lesson learned of the tragic firefight at Isa Khel, the German Army also changed the training of its light infantry units. Future contingents of paratroopers were trained in heavy, armored infantry tactics and cooperating with *Panzergrenadiers* before their deployment.[17] Such training before was solely limited to the *Panzergrenadiers*.

In the aftermath of Isa Khel the German Minster of Defense zu Guttenberg ordered three heavily armored self-propelled artillery guns, the *Panzerhowitzer 2000* to be deployed immediately to Kunduz province.[18] In 2011 he ordered a further two of these gigantic self-propelled guns as a reserve to Kunduz province. Even though considered one of the currently most advanced artillery systems worldwide, the *Panzerhowitzer 2000* was originally designed for the Cold War battlefields. With its maximum weight of 56 metric tons it defies current doctrines of light and highly expeditionary forces.[19] Undoubtedly the deployment of this massive Cold War artillery has shown the limits and difficulties of such "old" heavy armor, as one entire gigantic Russian *Antonov 124-100* airplane was necessary for just two such artillery systems.[20] Nonetheless, this piece of seemingly outdated Cold War equipment has proved its value for the ISAF troops in Kunduz province. Support with highly explosive grenades, exercise grenades (with limited explosive effect, e.g. if proximity to civilian areas makes the use of regular explosive ammunition too risky) fog screens and illumination projectiles[21] proved to be immensely beneficial support to the local ISAF forces.[22] This support was delivered substantially faster

---

[11] Id.

[12] *Afghan soldiers killed in friendly fire*, (from April 03, 2010), http://articles.cnn.com/2010-04-03/world/afghanistan.friendly.fire_1_gen-eric-tremblay-afghan-defense-ministry-german-troops?_s=PM:WORLD (last visited on Feb. 5, 2011).

[13] Id.

[14] *Germany Takes Over Quick Reaction Force in Afghanistan* (from June 30, 2008), http://www.dw-world.de/dw/article/0,,3451110,00.html (last visited Feb 6, 2011).

[15] *Schützenpanzer Marder: Das 20-Millimeter-Argument*, German Army Homepage (July 16, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W287EAH5365INFODE/content.jsp (last visited Dec 31, 2010).

[16] Id.

[17] Id.

[18] *Truppenbesuch im Norden des Landes: Guttenberg will Truppe in Afghanistan besser ausstatten (*from April 14, 2010), http://www.tagesschau.de/ausland/guttenbergafghanistan102.html (last visited Feb. 7, 2011);

[19] *Panzerhaubitze 2000* (homepage of the German army with the basic technical data without providing any specific date of the contribution), http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/NYvLCsIwEEX_aCYNSIuuFBFEqEttd2k6tEObB2GqIH68ycJ74GwOF3vMePPiyQgHb1Z8Ymd5P7xhJkogZGfPCywkQjCbbWD5kFZK4aNcjYuHkcAGT1Is5IWzp2QkJIghyVrKlIIuwCN2qjqf1E79V33rum_am9bNtb3cMTp3_AHdZdGo/ (last visited Feb. 7, 2011).

[20] *Eiserne Reserve für Kunduz*, (from Jan. 28, 2011); http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/NYzBCsIwEET_aDcRiuLNUAU96FHrbU1DE5smZdnoxY83FZyB4cEMg3esTvQKA0nIiSLesLNh-3iDd46BRikuRkhkPQfrxSV4kueV0rpCKvRDvC4_vQObk5Ml61BCzYFJMsOcWeLSFObaQOixU7o1qIF_6c-mPe2NWTfqeD5ccJ6m3RegFaEg/ (last visited on Feb. 7, 2011): the article describes the deployment of two additional reserve artillery pieces to Kunduz province in addition to the three already stationed there.

[21] *Team und Technik der Panzerhaubitze* (from July 23, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W287LJGW809INFODE/content.jsp.html (last visited Feb. 7, 2011): this article described the technology of the artillery piece and the different sorts and uses of ammunition.

[22] *Afghanistan: Einsatz der Panzerhaubitze 2000* (from Aug. 5, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W28829RC123INFODE/content.jsp.html (last visited on Feb.6, 2011): this article described the support of American ISAF forces by illumination rounds by the *Panzerhowitzer 2000*; *Afghanistan: Panzerhaubitze gegen gegnerische Kräfte eingesetzt* (from Nov.

(and considerably cheaper) than any close air support (CAS).

Another interesting comeback with the German armed forces was that of the old Cold War assault rifle HK G-3 which had already been replaced by the more modern HK G36 rifle. However, as the "old" HK G-3 assault rifle with its 7.62 mm caliber showed a far greater penetration power than the modern (and considerably more precise) modern HK G-36 (made mostly of carbon composite materials and advanced sights) with its 5.56 mm caliber. Therefore, the German ISAF contingent currently uses a mix of both assault rifles for its infantry units.[23]

The latest large scale Lebanon Campaign of the Israel Defense Forces (IDF) showed[24], that even an Army that has been honing its *counterinsurgency* and *counterterrorism* skills since the last full scale Israeli-Arab conflict in 1973, suddenly can be put in a situation of using more "old fashioned" large scale operations. Moreover, the conduct of the Lebanon campaign showed that after years of practicing solely *counterinsurgency* and *counterterrorism,* crucial military *core business* skills such as the combined arms warfare (the cooperation of the various branches of the army such as infantry, artillery, tanks etc.) are substantially weakened if neglected.[25] Losing such core capabilities can prove to be disastrous for any army committing the fallacy of presuming that present day warfare is the only type of warfare for future conflicts.

Thus, it is imperative to any security and defense policy to prepare for both: the kind of warfare the strategic establishment assumes (or desires) to be the likely future scenario *and* those scenarios found to be "unlikely" at present.

2. Developed country's demographics and obesity as a risk to national security-A return to the draft in the foreseeable future?

An issue less frequently referred to as a risk to national security is the issue of demographics and the epidemic of child and adolescent obesity.

Germany was the last of Western Europe's major powers to announce the abolishment of the draft/mandatory military service for June 2011.[26] Think tanks such as Stanford based *Center for International Security and Cooperation* (CISAC) are rather quick to conclude that at present such a draft would neither be politically feasible nor would a resulting large scale army be needed.[27] This, however, says little about the foreseeable future when an increasingly aging population, especially in Europe, might again necessitate such a draft – provided that societies do not want to resort to overt mercenary armies largely composed of foreigners or even larger involvement of private military firms (PMF).[28]

An increasingly recognized issue for national security is the vastly increasing percentage of obesity amongst children and young adults, which has become

---

1, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W28ASHXK951INFODE/content.jsp.html (last visited on Feb. 6, 2011): this article describe the use of the *Panzerhowitzer 2000* in the support of ISAF forces;

[23] Stephan Löwenstein, *Mit großem Kaliber gegen die Taliban*, (from July 12, 2010), http://m.faz.net/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc~E25ADC365E957456A99044E4C979A918A~ATpl~Epartner~Ssevenval~Scontent.xml (last visited on Feb. 7, 2011).

[24] David E. Johnson*, Military Capabilities for Hybrid War Insights from the Israel Defense Forces in Lebanon and Gaza*, RAND Corporation Occasional Papers (2010) at 2-3:

> The Israelis were very successful at LIC in the years before the Second Lebanon War, suppressing the intifada and dramatically lowering Israeli casualties. Unfortunately for Israel, as operations in Lebanon in 2006 would show, the Israeli Army's almost exclusive focus on LIC resulted in a military that was largely incapable of joint combined arms fire and maneuver… Eventually, Israeli ground forces entered Lebanon, where they had real difficulties, well documented in Matt Matthews's *We Were Caught Unprepared*… defeating Hezbollah required joint combined arms fire and maneuver, something the IDF was largely incapable of executing in 2006. Fire suppresses and fixes the enemy and enables ground maneuvering forces to close with him. Fire also isolates the enemy, shutting off lines of supply and communication and limiting his ability to mass. Maneuver forces enemy reaction. If the enemy attempts to relocate to more favorable terrain, he becomes visible and vulnerable to fire. If he remains in his positions and is suppressed, he can be defeated in detail by ground maneuver. Thus, hybrid opponents like Hezbollah demand integrated joint airground-ISR capabilities that are similar to those used against conventional adversaries, but at a reduced scale. Finally, the IDF's highly centralized C2 system, which had been effective in confronting the intifada, proved problematic against Hezbollah…

[25] Which in German military doctrine is called fittingly "Gefecht der verbundenen Waffen", i.e. "the combat of connected /joined weapons").

[26] *Military Reform: Conscription in Germany to End Next Summer,* DER SPIEGEL, Nov 23, 2010, http://www.spiegel.de/international/germany/0,1518,730660,00.html (last visited Dec. 31, 2010).

[27] See discussion hosted by CISAC at Stanford from Dec. 7, 2010, recorded under http://cisac.stanford.edu/news/the_ethics_of_the_draft_20101207/ (last visited Dec. 31, 2010); This fear of a large scale army neglects the possibility of a lottery system draft which would at least potentially make the entire military aged population liable to military service.

[28] To be sure, Europe and the whole developed (Western) World is not alone with the problem of aging societies as China's estimated fertility rate per woman is 1.6 children, well below the 2.1 needed to keep a population stable, and there may be other factors reining in China's population. Some predict that up to 30 million Chinese men won't have brides available to them by 2020 because the policy spurred selective abortion of girls. Others worry about the economic effect the policy will have, given an aging population. However, given the sheer size of the Chinese population this should still not lead to a server shortage of military aged men and women, see: Dan Murphy, *Suicide attacks down, Predator drone exits, and other overlooked stories in 2010* (Dec 22, 2010), http://www.csmonitor.com/World/Global-Issues/2010/1222/Suicide-attacks-down-Predator-drone-exits-and-other-overlooked-stories-in-2010 (last visited January 6, 2010).

the leading reason for the medical rejection of recruits. It is currently estimated that more than a quarter of all Americans aged 17 to 24 were unfit for service due to obesity.[29]

This constitutes a multi-facetted challenge for libertarian societies where mandatory exercising and banning of certain food items is not an option. Assuming educative campaigns are successful; this problem will endure for a substantial period of time.

A further demographic challenge to many developed (especially Western) societies is the difficulty to recruit the brightest university graduates for a career in the armed forces, especially in areas like computer science, which offer high-paying civilian career perspectives.[30] Especially for Western countries which are already burdened by a general aging and shrinking (military age) population this serious recruitment challenge is concerning. This problem is further aggravated in the context of non-Western countries with very developed cyber-warfare capacities, such as China, being able ensure through conscription that their brightest computer science students are at least temporarily contributing to their military's cyber-warfare capacities rather than joining high-paying jobs with companies such as *Google* or *Facebook* directly after leaving university.[31]

With the cyber-warfare arms race already having started, particularly by states that are disadvantaged in their conventional warfare capacity, the cyber-warfare capability of Western countries might crucially depend on enrolling some of its brightest minds in computer science either through conscription or through substantive, likely financial, incentives currently not available for military service.

---

[29] Alex Spillius in Washington, *Obesity among US schoolchildren 'a risk to national security'* (Apr. 25, 2010), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7632462/Obesity-among-US-schoolchildren-a-risk-to-national-security.html (last visited Dec. 31, 2010)

[30] Kevin Poulsen, *Air Force Launches Recruitment Campaign Touting Cyber Command*, (from Feb. 27, 2008), http://www.wired.com/threatlevel/2008/02/air-force-launc/ , (last visited on Feb. 5, 2011); Keith Epstein/Brian Grow, *Recruiting for the Cyber Wars Uncle Sam wants you—to help defend against Internet threats. But is the military any place for slackers and hackers?* (from April 15, 2008), http://www.businessweek.com/bwdaily/dnflash/content/apr2008/db20080414_422082.htm (last visited on Feb. 5, 2011); Tim Kane, *Why Our Best Officers Are Leaving*, The Atlantic, Jan./Feb.2011, http://www.theatlantic.com/magazine/archive/2011/01/why-our-best-officers-are-leaving/8346/1/ (last visited on Feb. 5, 2011); additionally in the popular surveys addressing the "best places where to start a career" it would be rather difficult to see the military mentioned among the top 100 ranks (when even Teach for America is mentioned there as one of the few NGO/Government Jobs), see e.g.:
Best Places to Launch a Career 2008 by Business Week, http://www.businessweek.com/interactive_reports/career_launch_2008.html , (last visited Feb. 5, 2011); *Best Places to Launch a Career 2009* by Business Week, http://www.businessweek.com/interactive_reports/career_launch_2009.html, (last visited on Feb. 5, 2011).

[31] *PLAN Conscripts Conscription Process*, http://www.globalsecurity.org/military/world/china/plan-personel-enlistedforces-conscripts.htm (last visited January 6, 2011); an interesting advertisement of the story of a Chinese student returning from his studies in Canada to join the Chinese armed forces can be found on an English speaking webpage apparently affiliated with the Chinese Army: *Wang Feilin's conscription story* (2010-Jan 12, 2010, 8:58 pm), http://www.chnarmy.com/html/2010-12/8384.html (last visited January 6, 2011); John Markoff et al., *2 China Schools Said to Be Tied to Online Attacks,* NY TIMES (February 18, 2010), http://www.nytimes.com/2010/02/19/technology/19china.html (last visited January 6, 2011); *Chinese army must deal with cyberwarfare: state media*, http://www.physorg.com/news/2010-12-chinese-army-cyberwarfare-state-media.html (last visited January 6, 2011); *CYBER WARFARE Risking chaos in the sky,* http://www.propilotmag.com/archives/2010/Apr%2010/A2_Cyberwarfare_p3.html (last visited January 6, 2011); *Chinese army to recruit university students*, http://www.study-in-china.org/ChinaEducation/PolicyLaws/20091112128115129.htm (last visited January 6, 2011); The "Active-Duty Officer's Law" and the "Regulations on the Appointment and Dismissal of Officers in Active Service" provide for standard performance appraisal based on evaluations by senior officers, a unit's political officer, and officer peer reviews. In some cases, evaluations combine such appraisals with objective examinations on subjects ranging from military technology to foreign languages to computer science, see: THE "PEOPLE" IN THE PLA: RECRUITMENT, TRAINING, AND EDUCATION IN CHINA'S MILITARY, (Roy Kamphausen et al. eds., Strategic Studies Institute, at 10, U.S. Army War College, 2008); Id. at 33: "…most of the PLA's educational institutions now offering graduate courses.33 Other curriculum changes were introduced in 1987 with the Interim Regulations on academic work. One important change was to broaden the focus of technical classes to expose students to a wider range of topics, and greater efforts were made to combine technical and command training. In addition, new kinds of courses have been added to the curriculum of many military academies, including military education theory, military psychology, foreign policy, international relations, management, and computer programming…"; Id. 109-:… College Students Entering the PLA:…Since the turn of the century, the PLA has tried to attract more college educated people into its ranks, not only as officers but also as NCOs and conscripts. So far, the number of college students entering the military as privates is relatively small; According to a 2006 *Xinhua* report, "more than 10,000" college students have entered the Army in the 5 years this policy has been in effect.16 Nonetheless, this trend appears to be on the rise, as 2,850 undergraduates from 73 institutions of higher learning in Beijing alone were reported to have volunteered for the Army in 2006…; Id. 298: Curriculums: To educate the "new-type military talent," curriculums of the command colleges have also undergone major changes… courses on space operations, cyber-space operations, counterterrorism, military-operations-other-than-war, peacekeeping, and international law have also been added…; *US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears*, The Guardian, 4 December 2010, http://www.guardian.co.uk/world/us-embassy-cables-documents/214462?INTCMP=SRCH (last visited January 6, 2011); The emphasis on information warfare has forced the PLA to recruit from a wide swath of the civilian sector, according to the report. As is the case with the U.S. military and its new Cyber Command, the PLA looks to commercial industry and academia for people possessing the requisite specialized skills and pasty pallor to man the keyboards. And although it hints broadly at it, the report offers no evidence of ties between the PLA and China's hacker community, see: Mark Rutherford, *Congressional commission focuses on China's cyberwar capability* (Oct 22, 2009 5:03 PM), http://news.cnet.com/8301-13639_3-10381621-42.html (last visited January 6, 2011).

3. Not *Vietnamization, Iraqization,* or *Afghanization* as Western Exit Strategies but "Technologization"/"Mechanization":

Prior to the "*Surge*" in Iraq in 2007 "Iraqization"[32] was the new buzzword that was enthusiastically used by strategists trying to find a solution to the "quagmire"[33] of the very critical situation in Iraq.

Increasingly with all major European military announcing concrete or vague but certainly definite draw-down dates for their forces in Afghanistan the word of Afghanization[34] has surfaced, albeit not as prolifically used as the "Iraqization" or "Vietnamization"[35] of earlier times.

However, when revisiting the history of the involvement of the United States in Vietnam and of the Soviet Union in Afghanistan it becomes questionable if this strategy of a sudden draw-down/retreat of forces and propping up of unpopular governments and their often ill-trained and ill-disciplined local security forces could realistically result in stable countries able to defeat insurgencies or military incursions.[36]

Western societies are known for their casualty wariness. For example, casualty aversion was very consciously exploited during the genocide in Rwanda when Belgian soldiers were slaughtered by Hutu militias[37], a lesson well learned by the militias from the UN mission in Somalia when the death of 19 US Soldiers during the *Battle of Mogadishu*[38] prompted the U.S. and the other involved Western Countries to abandon the mission in Somalia and draw back their troops. This demonstrates that missions to provide assistance to governments and their security forces cannot be sustained indefinitely at a certain intensity of conflict.

---

[32] Larry Diamond/James Dobbins et al., *What to do in Iraq: A Roundtable,* FOREIGN AFFAIRS, July/August 2006, http://www.foreignaffairs.com/articles/61745/larry-diamond-james-dobbins-chaim-kaufmann-leslie-h-gelb-and-ste/what-to-do-in-iraq-a-roundtable (last visited on Feb. 5, 2011); *Iraq: The Way Forward—Assessing Iraqization* [Rush Transcript; Federal News Service, Inc.], COUNCIL ON FOREIGN RELATIONS, (from March 20, 2006), http://www.cfr.org/iraq/iraq-way-forwardassessing-iraqization-rush-transcript-federal-news-service-inc/p10216 (last visited Feb. 6, 2011); Stephen Biddle, *Seeing Bagdad, Thinking Saigon,* FOREIGN AFFAIRS, March/April 2006, http://www.foreignaffairs.com/articles/61502/stephen-biddle/seeing-baghdad-thinking-saigon (last visited Feb.6, 2011).

[33] Another, almost iconic word of the Vietnam era, enthusiastically used by American and foreign opponents of the wars in Iraq and Afghanistan alike: David Rudenstine, *Vietnam: 'Quagmire' Quackery*, THE NATION, March 5, 2001, web edition: http://www.thenation.com/article/vietnam-quagmire-quackery (last visited on Feb. 4, 2011); Jeffrey Record/Andrew Terril, *Iraq and Vietnam: Differences, Similarities, and Insights*, (from May 2004), http://www.strategicstudiesinstitute.army.mil/pubs/summary.cfm?q=377 (last visited Feb.3, 2011).

[34] Gilles Dorronsoro, FIXING A FAILED STRATEGY IN AFGHANISTAN, THE HUFFINGTON POST (from Nov. 18, 2009, 4:27 PM), http://www.huffingtonpost.com/gilles-dorronsoro/fixing-a-failed-strategy_b_362720.html (last visited Feb. 1, 2011).

[35] Robert H. Johnson, *Vietnamization: Can it work?,* FOREIGN AFFAIRS (from July 1970), http://www.foreignaffairs.com/articles/24176/robert-h-johnson/vietnamization-can-it-work (last visited on Feb. 5, 2010); *The World: What It Means For Vietnamization*, TIME Magazine (from Mon., Apr. 5, 1971), http://www.time.com/time/magazine/article/0,9171,876901,00.html (last visited on Feb. 4, 2011).

[36] Certainly when neither the security forces have achieved a sufficient level of training nor basic civil society institutions have been properly developed.

[37] A staggering, very personal account of the Rwandan Genocide and the slaughter of the Belgian soldiers can be found in the book by the former commanding general of the ill-fated United Nations Assistance Mission for Rwanda (UNAMIR): ROMÉO DALLAIRE, SHAKE HANDS WITH THE DEVIL: THE FAILURE OF HUMANITY IN RWANDA (2003) at p. 255:"It slowly resolved in my vision into a heap of mangled and bloodied white flesh in tattered Belgian para-commando uniforms. The men were piled on top of…"; A further standard work on the Rwandan genocide is the book: PHILIP GOUREVITCH, WE WISH TO INFORM YOU THAT TOMORROW WE WILL BE KILLED WITH OUR FAMILIES: STORIES FROM RWANDA (1998), at p. 150 "…Belgium withdrew from UNAMIR-precisely as Hutu Power had intended it to do. Belgian soldiers, aggrieved by the cowardice and the waste of their mission, shredded their UN berets on the tarmac of Kigali airport…The desertion of Rwanda was Hutu Power's greatest diplomatic victory to date and it can be credited almost single-handedly to the United States. With the Somalia debacle still very fresh, the White House had just finished drafting a document called Presidential Decision Directive 25…"; Sarah B. Sewall, *U.S. Policy and Practice Regarding Multilateral Peace Operations,* CARR CENTER FOR HUMAN RIGHTS POLICY WORKING PAPER 01-3, 2000, http://www.hks.harvard.edu/cchrp/Web%20Working%20Papers/PKO.pdf (last visited on Feb. 7, 2011): "…While PDD 25 as a policy still called for strengthening UN peacekeeping, the Administration encountered increasingly less political room to maneuver… Congressional antipathy toward peace operations congealed during the first year of the Clinton Administration. By late October 1993, Somalia had become the poster child for the failure of UN peacekeeping. Many Members, and particularly Republicans, feared that the Administration's peacekeeping policy was too proactive, overly supportive of the UN, and divorced from U.S. national interests…"

[38] *Fire Fight From Hell*, NEWSWEEK (Oct. 18, 1993), http://www.newsweek.com/1993/10/17/fire-fight-from-hell.html# (last visited on Feb. 6, 2011); George J. Church & Michael Duffy et al., *Somalia: Anatomy of a Disaster,* (Mon. Oct 18, 1993), http://www.time.com/time/magazine/article/0,9171,979399-9,00.html (last visited on Feb. 5, 2011): …" The later multinational operation was to have been the forerunner of a new kind of U.N. intervention, one mounted not to monitor a peace but to establish one, undertaken without the traditional invitation from a host government and carried out not by the usual lightly armed troops but by forces toting enough weapons to fight a serious battle.
But it now seems possible that Somalia will set a very different precedent -- of extreme U.S. reluctance to mount or join any peacekeeping operation except one that poses little or no risk of casualties…"; Evan Thomas, *Their Faith And Fears*, (Sept 9, 2002), http://www.newsweek.com/2002/09/08/their-faith-and-fears.html (last visited on Feb. 7, 2011): "…The Washington national-security establishment had become risk averse after the end of the cold war. Pace knew it firsthand: he had been deputy commander of U.S. troops in Somalia after the Battle of Mogadishu in 1993. "We were told to circle the wagons and not get Americans hurt…"

Casualty and war wariness contributes to the increased use of drones and radio controlled robots over the recent years.

Although ever expanding in their capabilities, such remote controlled devices are still mostly used for combat support roles – mainly reconnaissance and bomb defusing.[39] So far only the United States possesses a substantial number and various types of drones capable of being used in combat roles, which are increasingly used against suspected militants in Pakistan and Afghanistan.

As the steeply increased number of drone attacks in Pakistan and Afghanistan shows, it is only a question of time until there will also be unmanned vehicles operating on the ground and in part taking on the role of infantry men in fully fledged combat roles.[40]

It is conceivable that in the not too distant future such ground operating fighting vehicles (unmanned ground vehicles [UGVs]) can be air dropped together with a large number of low-priced sensors. This large number of small, economical sensors, operating as a network, could by infrared, thermal or audio-sensors used to locate enemy sniper positions and relay them to the ground operating fighting vehicles. Either radio operated by a soldier or autonomously operating[41], this technology could be used to engage snipers without putting any soldiers at risk.[42]

How to program such autonomous fighting vehicles is an entirely different, complex ethical issue. For example, what kind of ethics would need to be used: act utilitarian ethics or consequentialist utilitarian ethics? Concretely, such decisions would be used to determine what kind of ethical calculus an autonomously operating combat robot would use if it were to confront Osama Bin Laden surrounded by infant human shields. What would be the program's core value on how many innocent infant/civilian lives Osama Bin Laden was worth: 10? 20? 100? 1000? Would the calculus be different for slightly lower value targets such as Mullah Omar or Ayman Muhammad Rabaie al-Zawahiri? Could there be an "IF" condition used in the robot's computer code that would transfer control back to a human operator in situations of such difficult ethical constellations? If such a transfer to a human operator is feasible or practical under hectic battlefield conditions remains an entirely separate question. A "practicality" "IF" condition would be a further colossal coding challenge. While Isaac Asimov's famed three robotic laws[43] provide good guidance in the context of all conceivable civilian uses, it remains unclear how they could be adapted in a military context, as the "no harm to humans" principle would be difficult to uphold in a situation.[44] Possibly, the three robotic laws could be still upheld if autonomously operating combat robots were only allowed to target vehicles, buildings or caves (possibly even with humans inside), but would never be permitted to target humans in a "face-to-face" confrontation. The debate on Asimov's robotic laws, even in a military context, was revitalized, when a South African Army robot killed seven South African soldiers during a test exercise.[45]

The question of individual criminal responsibility under International Humanitarian Law (IHL) and law of armed conflict (LOAC) for acts committed by the autonomously operating robot is so far barely addressed by the scholarly literature. A leading thinker in the field, Ron Arkin of Georgia Tech, introduces the very helpful starting point of assigning responsibility to one operator for the mission of an autonomous robot.[46] The operator

---

[39] Cassandra A. Fortin, *Airman and his robot a bomb defusing team* (June 2, 2010), http://www.northwestmilitary.com/news/focus/2010/06/northwest-military-ranger-newspaper-mcchord-airlifter-airman-robot-bomb-defusing-team/ (last visited January 6, 2011); http://www.irobot.com/gi/ (last visited January 6, 2011); Erik Sofge, *Robotic Task Force: A Two-Robot, Bomb-Defusing, Riot-Controlling, Firefighting Team* (October 1, 2009 12:00 AM), http://www.popularmechanics.com/technology/engineering/robots/4313799 (last visited January 6, 2010).

[40] Pam Benson et al., *Intelligence, potential plot are factors in drone-attack increase- Administration's Evolving Counterterrorism Campaign Has Widened Assault with Greater Regional Cooperation* (September 28, 2010), http://articles.cnn.com/2010-09-28/world/pakistan.drone.intel_1_drone-missile-attacks-pakistan-taliban?_s=PM:WORLD (last visited January 6, 2011); *Obama Has Increased Drone Attacks* (Feb 12, 2010), http://www.cbsnews.com/stories/2010/02/12/politics/main6201484.shtml (last visited January 6, 2011); Dan Murphy, *Suicide attacks down, Predator drone exits, and other overlooked stories in 2010* (Dec 22, 2010), http://www.csmonitor.com/World/Global-Issues/2010/1222/Suicide-attacks-down-Predator-drone-exits-and-other-overlooked-stories-in-2010 (last visited January 6, 2010); Rasool Daward, *Record Level Of US Drone Attacks Hit Afghan Militants* (September 15, 2010, 12:59 AM), http://www.huffingtonpost.com/2010/09/15/record-level-of-us-drone-_n_717557.html (last visited January 6, 2011).

[41] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 124-128 (2009)

[42] Apparently a robot currently being tested and called REDOWL (Robotic Enhanced Detection Outpost with Lasers) uses lasers and sound detection equipment to detect snipers…and instantly targets them with an infrared laser beam, see: P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 110 (2009)

[43] Apparently, these 3 laws were 1st introduced in Asimov's short story *Runaround* of 1942 and later elaborated in his *Robots* series (resulting in the popular movie *iRobot*). The content of these laws*:*

1.) A robot may not injure a human being or, through inaction, allow a human being to come to harm

2.) A robot must obey orders given it by human beings except where such orders would conflict with the First Law

3.) A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

[44] Some very good thoughts and basic sets of ethics instructions can be found in the work of Ron Arkin of Georgia Tech, such as: Ron Arkin, Governing Lethal Behavior in Autonomous Robots (2009) at p. 54 and 208.

[45] Priya Ganapati, *Robo-Ethicists Want to Revamp Asimov's 3 Laws*, WIRED, July 2, 2009, http://www.wired.com/gadgetlab/2009/07/robo-ethics/ (last visited Feb. 2, 2011).

[46] Ron Arkin, Governing Lethal Behavior in Autonomous Robots (2009) at p. 202.

would review and acknowledges the use of each obligation for the mission. The operator then confirms and types his name to accept responsibility for the conduct of the mission.[47] This is reminiscent of the command responsibility of officers for their soldiers and certainly addresses the issue of ethical conduct on operational level. However, the strategic level of the original programming/coding is not satisfactorily encompassed by this solution. The question of the individual criminal responsibility for the "collateral damage calculus" and computer code remains to be solved.

So far, developers and military planners are rather adamantly maintaining that ultimately humans will "stay in the loop."[48] However, the downing of Iran Air Flight 655 by a highly automated US destroyer's missile defense system or as the destruction of two allied planes during the second Gulf War by Patriot missiles show that already in many areas "the loop" of humans has been reduced to mere veto power. Therefore, the scenario of autonomous or at least "automatic" fighting robots might be closer than commonly assumed.[49]

Some military strategists assume that the speed, confusion and information overload of modern war will soon move outside of "human space."[50] The level of speed required on the battlefield certainly will increase beyond human capacity so that autonomously operating robots appear to be an inevitable development.[51] Some major military powers might have serious inhibitions regarding the use of such autonomous fighting systems. However the "prisoner dilemma" of "what if the other side gets it first" makes this inevitable development more likely. Thus, it is questionable if international treaty regimes banning such autonomous systems could be successful.

Before the large-scale introduction of autonomously operating robots becomes feasible, radio controlling robots will be the dominant means of operation.[52] The process of remotely controlling such robots will significantly differ from the button and joystick controlled present day approach. The progress made by brain controlled prosthetic limbs makes a scenario very probable where robots, capable of movement almost as precise as that of a human soldier, react to their controller's thoughts, which would provide such robots with previously unknown operational capabilities.[53]

In addition to the expanding combat roles of robots, their support roles will diversify and be capable of ever more complex operations such as Robotic evacuation vehicles which will be able to autonomously extract soldiers to safety and will enable human operators to conduct remote controlled surgeries inside the vehicle.[54]

Apart from conventional remote controlled robot, apparently recent *Defense Advanced Research Projects Agency* (DARPA) research has opened an alternative path, that of remote controlled animals such as in the so called "*robo*-rat" experiments.[55] In that experiment rodents were implanted electrodes in their brain through which the rats could be ordered to walk or climb through any path it was instructed to follow.[56]

As much as this would open up unknown capabilities to use such animals in mine-clearing or bomb detection operations, at the same time it raises considerable bioethics concerns regarding the morality

---

[47] Id.

[48] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 124-128 (2009)

[49] Id.; Similarly, Israel's newest "Iron Dome" rocket defense system is capable of taking out even very small incoming rockets and artillery shells and apparently operates as an automated system. Especially given the small size of Israel and the speed of the incoming rockets the margins of the response time needed are minimal and might proof to overwhelm human operators, see: *Iron Dome system passes final tests*, THE JERUSALEM POST July 19, 2010 8:56 PM, http://www.jpost.com/Israel/Article.aspx?id=181936 (last visited Feb. 9, 2011).

[50] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 124-128 (2009)

[51] Id.

[52] The possibility and feasibility of autonomously operating robots is mostly a question of the general progress of artificial intelligence (A.I.). Whilst in 1957 the AI crowd confidentially predicted that machines soon would be able to replicate all kinds of human mental achievements this turned out to be largely unachievable, in large part as the understanding of the human Brain is still limited. Most importantly, researchers noticed that they did not need to emulate human intelligence as a whole as intelligence revealed itself not to be a unitary thing but rather showed itself to be "all kinds of different" behaviors, see: Stephen Levy, *The A.I. Revolution*, WIRED, Jan. 2011, at 88; Thus, present day robotics follows this "insular" approach of certain kinds of intelligence(s). Often this type of AI is not even notice as such. Fittingly Google's cofounder Larry Page expressed that in 1978 typing queries into a machine and receiving access to all the world's knowledge would undoubtedly have been seen as a feat of AI[52]. The same applies to many present day personal robots who are able to "understand" and execute simple spoken commands, see: Stephen Levy, *The A.I. Revolution*, WIRED, Jan. 2011, at 88; interestingly by abandoning the old path of trying to emulate human intelligence we might be moving closer to true A.I. which in the foreseeable future might enable truly autonomously operating combat robots.

[53] JONATHAN MORENO, MIND WARS BRAIN RESEARCH AND NATIONAL DEFENSE, 39-40 (2006): In this book it is also described how a monkey succeeded controlling a robotic arm by a computer connected to his motor cortex. A group of Caltech scientists showed that intention can be read directly from activity in the parietal cortex.

[54] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 112 (2009)

[55] Unbeknownst to the general public worldwide and to large parts of the American public DARPA quite possibly constitutes one of the most important research funding entities on planet. Given its influence DARPA is exceptionally lean with a budget of only 3 billion USD when compared to an overall 651 billion USD spending on defense activities in the United States in 2009. Countless research programs on US university campuses are funded by DARPA, quite often unknown to the (PhD) students benefitting from DARPA funding. Founded in the wake of the *Sputnik* shock, DARPA has influenced technological revolutions for beyond the military sector and is e.g. responsible for the development of the internet, GPS navigation, the Worldwide Standardized Seismograph Network (WWSSN), staggering advances in prosthetic limbs etc., see: Michael Belfiore, The Department of Mad Scientists- How DARPA is Remaking Our World From the Internet to Artifical Limbs (2009).

[56] Id. at 43.

of brain-controlling living creatures in such a way. This is especially worrisome and bioethics-relevant as this research might open up possibilities control human soldiers in the same way.[57]

However, the increased use of such remotely operated or even autonomous vehicles (or animals) not suitable to win any hearts and minds for external assistance forces such as the International Security Assistance Force for Afghanistan (ISAF) or local government forces. Even in the absence of combat robots, the counter insurgency scholar David Kilcullen criticized that heavily armored presence in civilian areas lead to a very de-humanized perception of coalition forces in Iraq. In his book, *The Accidental Guerilla*, he described this as follows: "We are aliens-imperial stormtroopers with our Darth Vader sunglasses and grotesque and cowardly body armor…the insurgents have done to us what we said we would do to them-isolated us from the population by using the IED, and…our penchant for technology and fear of casualties…"[58]

If already the present human presence is capable of creating such a de-humanized "alien" perception the chances of a truly robotic force of winning over hearts and minds appear to be very slim.

Additionally, the use of such unmanned ground or aerial vehicles certainly will result in saving the lives of numerous soldiers and helps the local security forces buy some time until their own capabilities have increased. At the same time, these techniques will risk more civilian lives in the countries of origin of these foreign security forces. If militants in conflict areas such as Afghanistan will no longer be able in a position to inflict substantial casualties to the foreign assistance forces, they might find it necessary to increase strikes on civilians in the home countries of these highly technologized foreign forces.[59]

The attacks of September 11, 2001, the Beslan school siege[60], the Moscow theater hostage taking[61] or the Mumbai shootings provide a good glimpse of how such strikes might look like.[62]

Nonetheless, one should bear in mind that drones and radio controlled combat robots will most certainly be used by insurgents as their prices further decrease and as companies such as iRobot[63] and Robotex[64] have started pioneering robots for consumer (and law enforcement) use. Most prolific terrorist/insurgent organizations for all their anti-modernist and anti-globalization missions have shown to be very apt in putting the tools of globalization quite aptly to their use (e.g. internet and cell phones). The use of robots will not form an exception to this.

4. Creating a new breed of *Über*-Soldiers

In addition to the possibilities of the increased "outsourcing" of combat to remote controlled fighting vehicles a further (admittedly a bit more distant) development which needs to be contemplated by defense strategists are the numerous possibilities for the enhancements of the individual soldiers themselves.

E*xternal* enhancements of soldiers such as through exoskeletons[65] need to be contemplated just as much as *internal* enhancements of soldiers such as by the deliberate use of prosthetic limbs (which in the not too distant future might not only be able to compete with natural limps but exceed their capabilities.[66] The first

---

[57] Id. At 44.

[58] David Kilcullen, The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One (2009) at 136.

[59] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century (2009), p. 313: "…the more we take American soldiers of the battle fields, the more we will drive them to hit home…".

[60] Peter Baker and Susan B. Glasser, *Russia School Siege Ends in Carnage Hundreds Die As Troops Battle Hostage Takers*, THE WASHINGTON POST (from Sept. 4, 2004) at p. A01, http://www.washingtonpost.com/wp-dyn/articles/A58381-2004Sep3.html (last visited Feb.7, 2011).

[61] *Moscow Gas Debacle Leaves Putin Unscathed*, TIME homepage (from Monday, Oct. 28, 2002), http://www.time.com/time/world/article/0,8599,385038,00.html (last visited Feb. 8, 2011); Nick Paton Walsh & Jonathan Steele, *Chechen gunmen storm Moscow theatre-Chechen gunmen hold 700 hostages after storming Moscow theatre* (from Thursday October 24, 2002 02.36 BST); http://www.guardian.co.uk/world/2002/oct/24/russia.chechnya (last visited on Feb. 8, 2011).

[62] *Gunfire heard at two Mumbai hotels*, CNN WORLD homepage (from Nov. 26, 2008), http://articles.cnn.com/2008-11-26/world/india.attacks_1_mumbai-hotels-cama-hospital-indian-police?_s=PM:WORLD (last visited Feb. 8, 2011); *What we know about the Mumbai attacks*, CNN WORLD homepage (from Nov. 27, 2008), http://articles.cnn.com/2008-11-27/world/mumbai.investigation_1_cafe-leopold-oberoi-three-gunmen?_s=PM:WORLD (last visited Feb. 8, 2011); *The Mayhem in Mumbai Making sense of India's terrorist attacks,* NEWSWEEK homepage (from Nov. 26, 2008), http://www.newsweek.com/2008/11/25/the-mayhem-in-mumbai.html (last visited Feb. 8, 2011).

[63] http://www.irobot.com/ (last visited on Feb. 10, 2011).

[64] http://www.robotex.us/micro.html (last visited Feb. 10, 2011), for their robot AvatarMicro Robotex even posts credentials of an Oakland SWAT team officer on their homepage.

[65] Duncan Graham-Rowe , *MIT Exoskeleton Bears the Load Researchers have developed a motorless exoskeleton that can carry 80 pounds,* MIT TECHNOLOGY REVIEW (from Sept. 26, 2007), http://www.technologyreview.com/Infotech/19433/ (last visited Feb. 8, 2008);
Andrew Valiente, Design of a Quasi Parallel Leg Exoskeleton to Augment Load Carrying for Walking (August 2005) (Thesis for a Master of Science at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Institute of Technology): "…Exoskeletons have application for military and service personnel, as well as for patients with muscular impairments. Exoskeletons have the ability to traverse non-paved terrain accessing locations where wheeled vehicles cannot. Exoskeletons promise to allow people to run farther, jump higher, and bear larger loads while expending less energy. Recent physiological studies suggest that it may be possible to build an orthotic exoskeleton to dramatically increase the locomotory endurance of service personnel. Simulated reduced gravity experiments have demonstrated that the metabolic cost of walking and running can be reduced by 33% and 75% respectively, if gravity is reduced by 75%..."

[66] See the case of CAS 2008/1408/Pistorius v. IAAF/award of 16 May 2008, where a disabled South African athlete, a double amputee since he was 11 months old, who ran on two prosthetic legs known as "*Cheeta Flex*" sued for his right to compete in the 2008 Olympic games. The International Association of Athletics Federations (IAAF) had original had

steps are already being undertaken to enable the user to brain-control such limps[67]) or artificial retinas.[68]

Such enhancement are not only restricted to *mechanical* or *implantation of technical devices based* enhancement but could also include biological alterations such as by controlling soldiers' energy metabolism on demand (e.g. by inducing some kind of hibernation stage to seriously wounded soldiers).[69]

The legal and ethical implication for such developments are tremendous and have so far not sufficiently been reflected in the scholarly literature[70] and it remains uncertain how societies would react to a military caste or *de facto* species of soldier with genuinely distinguishable physical features (not dissimilar to soldier ants in many ant societies). The creation of such a *species/breed* of soldier would also raise challenges to democracy as such. The main challenge is twofold: How would such a caste of *Über*-soldiers see themselves and their loyalty to a democratic leadership and how careful or careless would the broader public vote on combat deployment of such a distinguishable species? Would the public be less concerned about a high rate of losses of such a distinguishable case?

The current situation of a widening "civil-military gap"[71] and the tendency that the military in most developed (especially Western nations) is increasingly being concentrated in *Mega*-bases[72] in thinly populated provincial areas (and thereby disappear out of society's sight) strongly suggests that with a distinguishable military species society would be significantly less concerned about the lot of their military caste.

The answers of societies to the "if" and "how" of such a new soldier species very much depend on the level of threat a society is faced with.[73] A society under an existential threat most likely will take a different position to such a soldier caste or species than a peacetime society not facing such existential threats.

However, such enhancement possibilities certainly are closer and less "science fiction"-like than they do

---

rejected his request and appeal based on IAAF Rule 144.2(e) states that "For the purposes of this Rule, the following shall be considered assistance, and are therefore not allowed: […] (e) Use of any technical device that incorporates springs, wheels, or any other element that provides the user with an advantage over another athlete not using such a device". The mere fact that it was even considered that this technical device would provide him with an advantage over able bodied athletes on the highest professional level clearly shows the tremendous progress made in the technology of such prosthetic limbs and that it might be probable that such prosthetic limbs might soon exceed natural limbs in their capacities.

[67] Henry T. Greely, *Law & the Revolution of the Neuroscience: An early look at the field,* Akron Law Review, 2009, at 698.

[68] Department of Ophthalmology School of Medicine and Hansen Experimental Physics Laboratory, Stanford University *Restoration of Sight to the Blind: Optoelectronic Retinal Prosthesis* http://www.stanford.edu/~palanker/lab/retinalpros.html# (last visited January 6, 2011).

[69] Jonathan Moreno, Mind Wars Brain Research and National Defense, 122 (2006)

[70] One of the laudable exceptions is Jonathan Moreno's Book: Id.

[71] Thomas E. Ricks, *The widening gap between the military and society: U.S. military personnel of all ranks are feeling increasingly alienated from their own country, and are becoming both more conservative and more politically active than ever before. Do they see America clearly?* THE ATLANTIC MONTHLY ELECTRONIC EDITION (from July 1997), http://www.theatlantic.com/past/docs/issues/97jul/milisoc.htm (last visited on Feb. 8, 2011); Thomas S. Szayna, Kevin F. McCarthy et al., *The Civil-Military Gap in the United States Does It Exist, Why, and Does It Matter?* Prepared for the US Army by RAND Arroyo Center (2007).

[72] Tadlock Cowan & Oscar R. Gonzales, *Military Base Closures: Socioeconomic Impacts,* CRS Report for Congress (Jan. 25, 2010); http://www.fas.org/sgp/crs/natsec/RS22147.pdf (last visited on Feb. 8, 2011); *Base Realignment and Closure (BRAC)*, http://www.globalsecurity.org/military/facility/brac.htm (last visited on Feb.8, 2011); Karen Jowers, AirForceTimes (from Monday Feb 7, 2011 15:50:14 EST), http://www.airforcetimes.com/news/2011/02/military-brac-bases-traffic-020711w/ (last visited on Feb. 8, 2011); *Bryan Bender*, Military cuts are sharpest in New England Officials worry for security, culture*, The Boston Globe April 10, 2005, http://www.globalsecurity.org/org/news/2005/050410-military-cuts.htm (last visited on Feb. 8, 2011): "New England has experienced a greater decline in military presence since the end of the Cold War than any other region of the country and is now at risk of losing its only active-duty air and naval bases, according to data compiled by the Globe and government officials. Thirty-five of 93 major bases shuttered across the nation since 1988, or a third of the total, were in Northeastern and Midwestern states, part of an exodus of large military installations from Northern states over the last decade and a half to the economically friendlier South and West. The six New England states saw the largest drop in active-duty personnel over the period. Nearly 60 percent of full-time military personnel based in the region went away as their installations were closed by decisions of four Base Realignment and Closure commissions, the last in 1995. In 1988, New England was home base for 30,600 active-duty personnel. It is currently home to less than 12,700. Now, New England is bracing to save the operational units that are left: its only remaining air base, in Brunswick, Maine, and only naval base, in New London, Conn… ''What concerns me is how the forces are moving to a red state-blue state bifurcation," said John Pike, a military scholar at GlobalSecurity.org in Alexandria, Va. ''Most of the bases are in the red states, and the bases in the blue states are mainly in red congressional districts. The military is a normal part of society in red states and not a normal part of society in many blue states…" "In Massachusetts alone, the number of military personnel dropped by 74 percent between 1988 and 2002, from 9,335 to 2,427, far higher than the 24 percent reduction nationwide, according to government statistics compiled by the Northeast-Midwest Institute, a military lobbying group. Maine had a 54 percent drop, from 5,849 to 2,689, according to the institute. The reduction was even more precipitous in New Hampshire, where the number of active-duty personnel in the state went from 4,143 to 326, a 92 percent drop and the largest slide in the nation. It was part of a wider trend. Across the entire Northeast the drop in military personnel was 37.5 percent. In the Midwest it was 46.6 percent. But the West only saw a 30 percent drop, while the South witnessed a mere 15 percent slide. ''There is an unmistakable societal consequence if we create a military without ties, in the form of active duty bases, in every part of the country," said Senator John F. Kerry, Democrat of Massachusetts…"*

[73] It remains a valid question where to draw a distinction between "artificial" enhancements and "natural" enhancements such as exercise, see also: JONATHAN MORENO, MIND WARS BRAIN RESEARCH AND NATIONAL DEFENSE, 133 (2006).

appear and therefore need to be addressed by the leading military scholars *before* they become reality.

5. The International Humanitarian Law (IHL) and Law of Armed Conflict (LOAC) implications of *cyber warfare* and anti-satellite warfare-Collateral damage beyond mere virtual damage & the new "mutual assured destruction" of the cyber-age:

Interestingly, some scholars who are deeply immersed in the topic of *cyber-attacks* or even *cyber warfare* appear to underestimate both the reality of cyber-warfare and its potential civilian collateral damages.

In a blog[74] published by the University of California in Berkeley, Stephen Maurer disputed a well-known computer scientist's complaint that cyber war was the "real WMD" and that America needed to spend less money on nuclear weapons defense.[75] Maurer attributed this WMD statement rather cursory to the fact that "people who spend weeks on end filling out grant applications are apt to say silly things."[76] Moreover, Maurer added that he had never heard anyone claim that Cyber War can inflict casualties on a nuclear scale. Additionally, the author raised the crucial question if cyber war qualified "as War on any scale at all."[77]

To Maurer problems only become "Wars" "when you run out of reasonable alternatives to calling in the military."[78]

Maurer disputed the validity of headlines of the Russia-Georgia conflict of 2008 such as "Cyber War is Official."[79] To Maurer instead of a cyber-war this conflict rather saw a number of "patriotic hackers" (= civilian amateurs or mobilized criminals) committing the same Cyber Crimes that the world's IT managers see on a daily basis.[80]

Maurer stressed that Microsoft received millions of error reports from users every day. However, he pointed out that in this case the number of eyeballs currently looking for vulnerabilities was incomparably larger than the world's population of Cyber Criminals and Cyber Vandals so that even State-funded searches became "a drop in the ocean."[81]

Maurer ended his reflection with the conclusion that certainly there was good reason that Defense Department should fund Cyber Crime research to protect its own systems and everyone else's. However, Maurer pointed out that this was already occurring in the *old* "cyber crime" context. To Maurer "cyber war" rhetoric constituted an unnecessary escalation – and an expensive one at that.[82]

Maurer's reflections were included in this paper, as he managed to muster a wide array of conceivable counter arguments to the reality of cyber warfare.[83] The limited concern assigned to cyber warfare in Maurer's blog reflected how to a large part of the general public cyber warfare still appears to have only virtual, i.e. cyber space ramifications,[84] seemingly without "real" work effects and damages.

This public underestimation of cyber warfare is bound to change after the highly effective "Stuxnet" computer virus attack on Iranian industrial and factory systems and which apparently targeted Busher nuclear

---

[74] "The Berkeley Blog-Topical Questions, Campus Experts and Public Opinion from UC Berkeley".

[75] Stephen Maurer, *Keeping the Cyber-Peace,* The Berkeley Blog, Topical Questions, Campus Experts and Public Opinion from UC Berkeley (Feb. 19, 2010), http://blogs.berkeley.edu/category/science/20091111/?full=1 (last visited Jan. 6, 2010).

[76] Id.

[77] Id.

[78] Id.

[79] Id. Maurer attributes this headline to *Aviation Week* in its edition from Sept. 14 2009.

[80] Id.

[81] Id.

[82] Id; Admittedly, Maurer's considerations have been assigned a rather large portion in this paper, especially given that he is not a leading scholar and as his position at the time of the drafting (in the last quarter of 2009) was a minority view in the scholarly literature and the public debate: Especially given that before the publication of Maurer's blog major military powers had publically admitted to take the threat of cyber war very seriously: Doug Tygar, *UCB leader in critical infrastructure protection research,* The Berkeley Blog, Topical Questions, Campus Experts and Public Opinion from UC Berkeley (Nov. 9, 2009), http://blogs.berkeley.edu/category/science/20091111/?full=1 (last visited Jan. 6, 2011): …Cyberwarfare is something that is taken seriously by the Chinese and Russian military. Officers in the (Chinese) People's Liberation Army have written treatises on cyberwarfare. And we have extensive evidence of successful penetrations of US governmental and military sites. The US also takes cyberwarfare seriously: Defense Secretary Gates announced on June 23rd a new "US Cyber Command" (part of the US Strategic Command). While protection of government and military computer systems is a priority of the first order, the US is even more vulnerable to electronic attacks on the civilian critical infrastructure. These attacks are not merely a hypothetical possibility, as President Obama discussed in his May 29 remarks…; Tim Reid, *China's cyber army is preparing to march on America, says Pentagon,* The Times-The Sunday Times (Sept. 8, 2007), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece (last visited Jan. 6, 2011); Spencer Ackerman, *It Begins: Military's Cyberwar Command Is Fully Operational*, (from Nov.4 2010), http://www.wired.com/dangerroom/2010/11/it-begins-militarys-cyberwar-command-is-fully-operational/ , last visited on Feb. 5 2010); The concern of major military powers with cyber warfare was strengthened, well before Maurer's blog, after the after severe cyber-attacks e.g. on Google, Intel, Adobe, the Dalai Lama's government in exile: Doug Tygar, *Cyberwar,* The Berkeley Blog, Topical Questions, Campus Experts and Public Opinion from UC Berkeley (Feb. 23, 2010), http://blogs.berkeley.edu/category/science/20091111/?full=1 (last visited Jan. 6, 2011)

[83] Interestingly even high ranking "cyber war" officials downplay the existence of something worthy the name cyber war: Ryan Singel, *White House Cyber Czar: 'There Is No Cyberwar'*, (from March 4, 2010), http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ , (last visited on Feb. 5, 2011).

[84] Monish Shah, *Shah: Prepare for cyber-warfare* (Nov. 12, 2010), http://www.yaledailynews.com/news/2010/nov/12/shah-prepare-cyber-warfare/ (last visited Jan. 6, 2011)

power plant has been described as one of the "most refined pieces of malware ever discovered."[85]

Experts described that the malicious software, first detected in June last year, was almost certainly designed to make damaging, surreptitious adjustments to the centrifuges used at Natanz, Iran's uranium enrichment site.[86] Separate investigations by US nuclear experts have discovered that "Stuxnet" worked by increasing the speed of uranium centrifuges to breaking point for short periods. At the same time it shut off safety monitoring systems, hoodwinking operators that all was normal.[87]

"Stuxnet" illustrates what has been largely neglected in both Law of Armed Conflict (LOAC) and International Humanitarian Law (IHL) both in the scholarly discussions and the curricula of military academies.[88] LOAC and IHL attempt to limit unnecessary suffering during armed conflicts. IHL is especially relevant for cyber warfare as IHL tries to protect the civilian population and to limit the damage to civilian infrastructure.

The "Stuxnet" cyber-attack demonstrates that the imperatives for proportionality in causing civilian harm are comparable to e.g. the bombardment of a bridge which has dual civilian and military use. In case of an attack on such a *dual use* target, it needs to be determined first if the target has a sufficiently important military use in order to justify an attack as such. Additionally, once it is determined that indeed the military use is sufficient to launch an attack, it needs to be determined what would be the number of expected civilian casualties and the expected damage to the civilian infrastructure. Once it is concluded that the reasonably expected civilian casualties and infrastructure damages are not disproportionate to the expected military gains in destroying the target, every precaution must be taken to minimize the probability of civilian casualties and destruction of civilian infrastructure.

Likewise in the case of cyber-attacks such as the "Stuxnet" operations the collateral damages of such a virtual attack need to be minimized. Even if the attack is "only" virtual, indiscriminate attacks can cause disproportionate civilian casualties and immeasurable damage to civilian infrastructure.

In the case of "Stuxnet" it is very probable that the "Stuxnet" virus constitutes an indiscriminate attack as it is not only capable of harming the suspected target, the Busher nuclear power plant's centrifuges, but also any industrial and factory systems. It is conceivable that this virus could also attack factories producing crucial medicines or life saving devices. The number of potentially resulting civilian casualties could theoretically be just as high as in the case of e.g. carpet bombing a bridge with dual civil military use.

The existing literature supports this view and stresses that even in the case of "only" virtual, i.e. cyber-attacks the known principles of *distinction*, as stipulated in Art. 48 Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) clearly states the imperative distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives. Additionally (Art. 51 AP I) stipulates that indiscriminate attacks are prohibited.

Indiscriminate attacks are:

"(a) those which are not directed at a specific military objective;
(b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
(c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;
and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."[89]

Apart from the indiscriminate nature and the high likelihood of civilian collateral damage (even if "only" in the form of exorbitant financial costs to the civilian population, whilst actual loss of life and limb certainly is not an unlikely result in such cyber-attacks) through such cyber-attacks the problem of proliferation arises. In the past the mere term and the legal regimes connected to

[85] Josh Halliday, *Stuxnet worm is the 'work of a national government agency' Malware believed to be targeting Iran's Bushehr nuclear power plant may have been created by Israeli hackers*, The Guardian (Sept. 24, 2010), http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency (last visited Jan. 6, 2011); *A cyber-missile aimed at Iran?* The Economist (Sept. 24, 2010), http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm (last visited Jan. 6, 2010).

[86] Christopher Williams, *Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel' A British security expert has uncovered new evidence in the Stuxnet virus attack on Iran's nuclear program*, THE TELEGRAPH, Jan. 21, 2011, http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html (last visited Feb. 8, 2011).

[87] Id.

[88] Which does not mean that there are no articles on this subject. To the contrary, there are a number of good recent articles on this subject, however, compared to the publication density of other areas of LOAC or IHL they are still comparably scarce: Eric Talbot Jenssen, *Cyber Warfare and Precautions Against the Effects of Attacks*, TEXAS LAW REVIEW, Jun 2010, 1522-1556L; Knut Dörmann, *Computer network attack and international humanitarian law*, *Extract from The Cambridge Review of International Affairs "Internet and State Security Forum"* (19 May 2001), http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm (last visited Jan 6, 2010); Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law*, *The Principles of Distinction in the Age of Cyber Warfare*, MICHIGAN LAW REVIEW Vol. 106, 1427, 1450 (2008); Dr. Rex Hughes, *Towards a Global Regime for Cyber Warfare*, Chatham House, London (2009).

[89] See also: Knut Dörmann, *Computer network attack and international humanitarian law*, *Extract from The Cambridge Review of International Affairs "Internet and State Security Forum"* (19 May 2001), http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm (last visited Jan 6, 2010).

"proliferation" seemed to be reserved to Weapon of Mass Destruction (WMD). With the advent of powerful cyber-attack programs such as "Stuxnet", the uncontrolled proliferation of such programs (whether in the form of worms, viruses or any other malware) the problem of "proliferation" also extents to these virtual "WMDs."[90]

"Stuxnet" spread far beyond its intended target to countries as distant as China and Germany, Kazakhstan and Indonesia.[91] This could support argument of the "Stuxnet" operation having been an indiscriminate attack which should be subjected to the same principles and prosecution as non-virtual attacks in IHL.

The same considerations for the IHL implications for cyber warfare clearly can be applied to satellite warfare as the consequences would be just as indiscriminate and potentially disastrous, especially as most satellites share the dual use characteristics of most cyber networks. The consequences of communication or navigation satellites being targeted and disabled[92] would be just as disastrous, as they could result in super tankers or planes crashing or colliding due to hampered navigation.

One mildly comforting fact remains for both cyber and satellite warfare. It appears to be immensely difficult to limit the effects and to provide effective protection against enemy attacks which poses the very real risk of mutual assured destruction.[93]

Most modern armies and societies are so dependent on the functioning of their information technology (IT) and their satellite technology, that any *cyber attack* and the following retaliation has the potential to be catastrophic on every fiber of the military machinery and society as a whole. It can therefore be presumed that all rational state actors are aware of such a very real possibility of mutual assured destruction and would be very much interested in limiting this tool of warfare. If the same would be true for isolated, totalitarian "rogue" states or desperate societies facing defeat remains to be seen.

While most major militaries even appear to have developed (highly classified) Rules of Engagement (ROE) for the use of cyber tools as a means of warfare, so far no overt or prominent "first strike"[94] vs. retaliation doctrine has emerged.

6. What does constitute an "armed attack" in *cyber*-space?

Directly related to these doctrinal issues and the topic "mutual assured destruction", it remains neglected *what* actually does constitute an all-out *cyber-attack*/use of force in cyberspace and *what* sets it apart from the scale and scope of a "normal" *cyber* vandalism. Concerning the wealth of doctrinal works surrounding the definitions of armed attack under Art. 51 Chpt. 7 of the UN Charter, works analogizing these doctrines to *cyber-attacks* are very scarce.

The Estonian and Georgian *cyber-attacks* from 2007 and 2008 have been a first test case further develop theories about *cyber-warfare* with the key questions being how to define it, whether to engage in it, and how to defend against it.[95] Some commentators argue that for a *cyber-attack* to qualify as "*cyber-war*" it would need to take place alongside actual military operations.[96] This can be analogized to the earliest operations against communications infrastructure. For instance during the American Civil War, a landing party from a Union navy steamer, went ashore to cut the telegraph lines between Fredericksburg and Richmond.[97] The Russian navy pioneered the use of radio jamming in the Russo-Japanese war of 1905. *Cyber-attacks* on infrastructure would constitute a further logical step in this tech warfare evolution.[98] The attacks on Georgia might qualify as *cyber-warfare* by this definition, but those on Estonia would not, since there was no accompanying military offensive in the real world.[99] Some commentators phrase this concept rather concisely as "For it to be *cyber-war*, it must first be war in first place."[100]

Many scholars do not concur with this condition. A "digital Pearl Harbor" is conceivable as an unexpected

---

[90] Gregg Keizer, *Why did the Stuxnet Worm spread? Propagation hints that first attack failed, say researchers* (October 1, 2010 01:02 PM)

[91] Id.

[92] Sharon Weinberger, *Return of the Killer Satellite Weapons* (April 23, 2007), http://www.wired.com/dangerroom/2007/04/return_of_the_k/ (last visited January 6, 2010).

[93] Reminiscent of KARLS JASPERS, THE ATOM BOMB AND THE FUTURE OF MANKIND, 1961; see also: http://plato.stanford.edu/entries/jaspers/ (last visited January 6, 2011); Colonel Charles Williamson, of the intelligence and surveillance division of America's air force, proposed that the United States should establish its own "botnet"—a network of machines "that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic." America, he wrote, "needs the ability to carpet-bomb in cyberspace to create the deterrent we lack." The botnet could be built out of obsolete computers that would otherwise be discarded, he suggested. Such as botnet would be an excellent tool to retaliate again an earlier all-out cyber attack, see: *Marching off to cyberwar he internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with "cyberwar",* THE ECONOMIST, Dec 4, 2008, http://www.economist.com/node/12673385?story_id=12673385 (last visited on Feb. 10, 2011).

[94] John King, *Bush outlines first-strike doctrine*, http://articles.cnn.com/2002-09-20/politics/bush.national.security_1_military-force-policy-attacks?_s=PM:ALLPOLITICS (last visited on Feb. 4, 2011); Ian Traynor, *Pre-emptive nuclear strike a key option, NATO told*, The Guardian, Jan. 22, 2008, http://www.guardian.co.uk/world/2008/jan/22/nato.nuclear (last visited on Feb. 5, 2011).

[95] *Marching off to cyberwar-The internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with "cyberwar",* THE ECONOMIST, Dec 4, 2008, http://www.economist.com/node/12673385?story_id=12673385 (last visited Feb. 10, 2011);

[96] Id.

[97] Id.

[98] Id.

[99] Id.

[100] Id.

attack on a nation's infrastructure via the internet, in which power plants are shut down, air-traffic control is sabotaged and telecoms networks are disabled.[101] This would not necessarily need to be accompanied by conventional warfare. As the *cyber-attack* alone could paralyze the targeted society (especially if the targeted society has a more powerful conventional military) there would be no need to reinforce it with conventional force.[102]

The strongest definition of *cyber-war* requires that *cyber attacks* cause widespread harm, rather than mere inconvenience. The Georgian attacks did not cause physical harm, unlike the military operations going on at the same time.[103]

All sorts of "translation problems" arise when trying to apply existing international rules relating to terrorism and warfare to online attacks.[104] The United Nations Charter prohibits the use of force except in self-defense or when authorized by the Security Council. However, as explained there is little doctrinal framework on what counts as "the use of force" in *cyberspace*.[105] Clarity is needed with concerns to the minimal threshold that needs to be crossed in order to constitute an *attack*. It can be debated if a Denial of Service (DoS) attack would cross that threshold.[106] Not only the *type* of attack needs to be contemplated but also *what* would be targeted: would an attack on the media sector suffice or would rather be an air controlling facility the target of the attack?[107] An interesting idea in this debated is the requirement that effects to be produced by a *cyber-attack* would constitute an armed attack if the same effects could only be produced by an all out conventional military attack.[108]

In the sense of Article 51 of the U.N. Charter, it is likely that the *cyber-attack* would be treated as an armed attack. Similarly, if a *cyber-attack* had the same effects and was otherwise similar to government-initiated coercive or harmful actions that are traditionally not treated as the "use of force,"[109] such a *cyber-attack* would likely not be regarded as an action justifying a use of force in response.[110] Such a "similar effect" (compared to a conventional attack) doctrine constitutes a helpful starting point in creating a new conceptional framework. However, this concept has its limits as it does not differentiate among the innate levels of danger of different targets effected (the previous example of media vs. air control facilities). Also, it makes it systematically difficult to separate the potential effects of a comparable conventional attack from the effects of other means short of armed attack. For instance, an argument could be made that the failure of a (coal burning) power plant due to a *cyber-attack* could have only been caused by a comparable conventional bomb raid on that power plant. However it is also imaginable that the same power cut could have been caused by a coal embargo which would have the same effect.

Reaching consensus on the threshold of an attack is crucial especially in the context of military alliances such as NATO where the member states are treaty-bound to respond to an attack on any of their members and might be able to turn a limited regional conflict into a substantially larger crisis.[111]

7. The *Black Swans* of defense policy-common statistical fallacies in the prediction of future threats to security:

As described under the first paragraph of this article, there appears to be overwhelming consensus that the future of military involvement belongs to operations in counterterrorism and counterinsurgency.

Without venturing into *Popperian*[112], *Kuhnian*[113] or Lacatosian[114] *meta*-theoretical considerations on the development of such widely shared theoretical assumptions the underlying paragraph reflects on their origins, their innate danger and why they are symptomatic for modern societies.

In this day and age widely shared assumptions and predictions of the celebrated "analysts" of all fields are firstly derived by the interpretation of vast amounts of data of past events. The obsession of modern day societies with gathering information and intelligence[115] leads to an immense number of data which is then extrapolated to make predictions on future events (or at least their likelihood).

The influence of the devoutness to these complex probabilistic systems[116] can be seen in every aspect of

---

[101] Id.
[102] Id.
[103] Id.
[104] Id.
[105] Id.
[106] Id.
[107] Id.
[108] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:63, 2010], p. 73, http://www.jnslp.com/read/vol4no1/06_Lin.pdf (last visited Feb. 10, 2011).
[109] Such as: economic sanctions, espionage, or covert actions such as planting information or influencing elections, see: Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:63, 2010], p. 73, http://www.jnslp.com/read/vol4no1/06_Lin.pdf (last visited Feb. 10, 2011).
[110] Id.
[111] Id.
[112] Karl Popper, The Logic of Scientific Discovery (1934); Karl Popper, Conjectures and Refutations: The Growth of Scientific Knowledge (1963).
[113] Thomas S. Kuhn, The Structure of Scientific Revolutions (1962).
[114] Lacatos argued that one research programme (i.e. a theory) can be described as progressive while its rivals are degenerating. A progressive research programme is marked by its growth, along with the discovery of stunning novel facts, development of new experimental techniques, more precise predictions, etc. A degenerating research program is marked by lack of growth, or growth of the protective belt that does not lead to novel facts: published in John Worrall & Gregory Currie (eds.) The Methodology of Scientific Research Programmes: Volume 1: Philosophical Papers (Philosophical Papers Vol. I), (1980).
[115] Drury D. Stevenson, *The Effect of National Security on the Criminal Law Paradigm*, Working Paper Series (September 1, 2010), http://ssrn.com/abstract=1669832 (last visited Feb. 8, 2011), at p. 3.
[116] Which at times appear to amount to little more than esoteric numerology.

modern societies, most notably in the financial markets, the insurance sector, criminal law policy (and the correctional system)[117] and defense policy.

Particularly highly developed societies show a strong obsession of avoiding uncertainty and trying to achieve the utmost risk minimization through their highly developed insurance sectors.[118] This basic tendency can be observed in all the aforementioned sectors and is fundamentally (re-) shaping them.

This reshaping is very prominent in the sector of criminal law. It is observed in scholarly literature that currently we are witnessing a shift toward focusing on incapacitation and prevention of crime rather than traditional deterrence or retribution.[119] Whereas the emphasis of criminal law in previous eras was punishing the blameworthy (retribution) or saving people from themselves (deterrence), the new focus is on preserving a comfortable, secure way of life, and law is approached as a method of eliminating risks.[120] When elements of deterrence are incorporated, the new paradigm shifts the focus toward lowering the rewards of illegal activity (by foiling terrorist plots or conspiracies before they succeed)[121] or raising the transaction costs[122] for criminals rather than traditional deterrence, which focused on the threat of punishment.[123]

Accordingly, in criminal law policy funding is allocated towards these large data analysis and to the incapacitation/prevention efforts found most efficient to maintain society's uncertainties and preserve a "secure" way of life.[124]

In the financial sector such number analysis and limitation of uncertainty has taken a dynamic of its own. Based on the analysis of vast amounts of data nowadays the complex models are being used by sophisticated programs and computers. These computers and programs are not limited anymore to "number crunching" but make actual decisions.[125] By some estimates computer aided high frequency trading now accounts for about 70% of total trade volume.[126]

What does this mean for defense policy, the interpretations and the predictions by the "analysts" and scholars? Most crucially, it can be noted that analysts and scholars cannot escape the background of the data and data-analysis obsessed societies that they are part of.

Therefore, it is hardly surprising that they apply the same tools and derive their predictions in the same fashion that for instance economists use in order to predict future developments in the markets.

The strength of developed societies and the whole data analysis culture lies in the substantial proficiency in managing the known risks.

However the *Achilles Heel* of such a model/culture lies in the unknown dangers, the *Black Swans*[127] of what can be expected based on experience and empirical knowledge.

Black Swan logic makes what you do not know far more relevant than what you do know.[128] One example is the terrorist attacks of September 11, 2001. Had the risk of a non-state actor launching an air attack of that magnitude been deemed *conceivable* and thus worthy of preventive action, the event would not have happened.[129] An additional example is the German invasion of France 1940. Based on their experiences with the German advances through Alsace-Lothringen in 1870 or Flanders in 1914 the French had built the famed fortified *Maginot* Line to prevent the same routes of attacks. The *Maginot* Line had one decisive gap at along the Ardennes as it was found inconceivable that any larger army, let alone a modern heavily mechanized army could advance through this hilly, forested area with its narrow roads. Yet that was exactly what the German army did.[130] Early reports by French reconnaissance airplanes on gigantic (and very vulnerable) German troop concentrations in the Ardennes were largely ignored.[131] The *Black Swan* of the "*inconceivable"* modus operandi of the German army led to the defeat of the

---

[117] Drury D. Stevenson, *The Effect of National Security on the Criminal Law Paradigm*, Working Paper Series (September 1, 2010), http://ssrn.com/abstract=1669832 (last visited Feb. 8, 2011).

[118] This observation was expressed by Prof. Drury D. Stevenson during the presentation of hiss paper *The Effect of National Security on the Criminal Law Paradigm* during the DEFENSE POLICY SYMPOSIUM on Jan. 22, 2011 at Stanford Law School.

[119] Drury D. Stevenson, *The Effect of National Security on the Criminal Law Paradigm*, Working Paper Series (September 1, 2010), http://ssrn.com/abstract=1669832 (last visited Feb. 8, 2011), p.9.

[120] Id.

[121] Id.

[122] Id. at p. 12; Airport checks are as well such instruments of incapacitation which considerably raise the transaction costs of would be terrorists.

[123] Id. at p. 9.

[124] Id. at p. 4.

[125] Felix Salmon & Jon Stokes, *Bull vs. Bear vs. Bot,* WIRED Jan. 2011, p.91.

[126] Id.; this prevalence of computer trading and automated decision making prompted the "Thinking machines" entrepreneur and MIT graduate William D. Hillis to the statement: "The computers are in control, we just live in their world".

[127] The "Black Swan" is a popular concept to illustrate the concept and problem of induction in logic courses in philosophy and mathematics. Until about the middle of the previous century induction was treated as a quite specific method of inference: inference of a universal affirmative proposition (All swans are white) from its instances (*a:* is a white swan, *b:* is a white swan, etc.) The method had also a probabilistic form, in which the conclusion stated a probabilistic connection between the properties in question. It is no longer possible to think of induction in such a restricted way; much synthetic or contingent inference is now taken to be inductive; some authorities go so far as to count all contingent inference as inductive, see: *The Problem of Induction*, STANFORD ENCYCLOPEDIA OF PHILOSPHY, *First published Wed Nov 15, 2006; substantive revision Mon Jun 21, 2010*, http://plato.stanford.edu/entries/induction-problem/ (last visited Feb. 9, 2011).

[128] Nassim Nicholas Taleb, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2007).

[129] Id., p. xxiii.

[130] Dr. Gary Sheffield, *The Fall of France,* BBC homepage series World Wars in-depth, last updated Aug. 9, 2010, http://www.bbc.co.uk/history/worldwars/wwtwo/fall_france_01.shtml (last visited Feb. 9, 2011).

[131] Julian Jackson, THE FALL OF FRANCE: The Nazi Invasion of 1940 (2003), p.42.

French army and the British expeditionary corps in just 6 weeks.[132]

The philosopher and statistician Nassim Nicholas Taleb in his bestselling book "THE BLACK SWAN: THE IMPACT OF HIGHLY IMPROBABLE" describes the pattern of "clustering" according to which journalists tended to cluster not necessary around the same opinions but frequently around the same framework of analyses.[133] According to Taleb they assigned the same relevance to the same sets of circumstances and divided their observations into the same categories.[134]

It is not improbable that such clustering is responsible for the widely shared believes of scholars and practitioners that for the foreseeable future counterinsurgency or counterterrorism are the only games in town. Every other "inconceivable" type or intensity of warfare has the possibility of being the next "Black Swan".

Referring to Bertrand Russel, Taleb describes the prolific philosophical question of how one could logically go from specific instances to reach general conclusions.[135] This is commonly referred to as the Problem of Induction or the Problem of Inductive Knowledge.[136] To illustrate this problem Taleb uses the turkey[137] analogy from Bertrand Russel according to which the turkey learned, based on its observation, it will receive an increased number of friendly feedings with every new day. As this has been its experience from the past 1000 days it is reasonable to assume that this will provide sufficient data to predict future developments.[138] However, on the 1000th day the unexpected happens to the turkey. It is remarkable that in this example the risk was the highest when the turkey's confidence was at its highest level as well.[139] This can be analogized to the nature of any prediction of future events based on the experiences with past events, albeit within the limitations of every analogy in relation to the reality it refers to.[140]

Nonetheless, with the intrinsic limitations of any analogy it is worth posing the hypothetical question who would be the turkey and who would be the butcher if the analogy were to be applied. Certainly the "surprise" will be on the turkey's and not the butcher's side.[141]

As a further example Taleb refers to the summer of 1982 when large American banks had almost their entire earnings wiped out. They had been lending to South and Central American countries that all defaulted at the same time.[142] This was described as an event of "exceptional nature"[143] and thus inconceivable.

Taleb stresses that due to the often slow nature of historical changes and technical implementations that "Black Swans" can be built up over decades (and seemingly gaining credibility with each day of being upheld) but be destroyed within seconds).[144]

Moreover, Taleb rejects the notion of *Knightian* risks (computable risks) and *Knightian* uncertainties (not computable) as he finds them to be "absent from real life" and "mere laboratory contraptions."[145]

To conclude this epistemological[146] reflection on the widely held predictions on the future of warfare, it needs to be emphasized that Taleb's considerations must not necessarily be true and all empiricism based predictions must not necessarily be false.

It was rather the intent of this section to provide one possible explanation of the origin and process of widely shared predictions.

Furthermore, it was the goal of this paragraph to impose some critical reflection on the aura of certainty surrounding many scholars and decision-makers regarding their ability to accurate predict future developments. Undoubtedly, the lessons to be learned from past developments should be crucial factors in determining future defense and security policy for probable events on the horizon. However, it should always be the imperative of defense and security planning to be prepared for the "unlikely" and inconceivable events. This is especially true if the capabilities required for these "improbable" scenarios are very complex and likely to be lost if not practiced on a regular basis or not being assigned sufficient funding.

[132] Id. p. 2.
[133] Id. p. 15.
[134] Id. p.15.
[135] Id., p. 40.
[136] Id., p. 40.
[137] Id. 40: For the sake of accurateness: Russel used a chicken in his original analogy instead of a turkey.
[138] Id. 41.
[139] Id. 41.
[140] As obviously one could make the argument that the experience, the data and number of sources and witnesses in the security policy context are incomparably larger than in the turkey example.
[141] Id. p. IV: Taleb words this as follows: "…A *Black Swan* for the turkey is not a *Black Swan* for the butcher…"
[142] Id. p.43.
[143] Id. p. 43.
[144] Id. p.44.
[145] Id. p.128.
[146] *Epistemology,* STANFORD ENCYCLOPEDIA OF PHILOSOPHY *(*First published Wed Dec 14, 2005), http://plato.stanford.edu/entries/epistemology/ (last visited Feb. 8, 2011).