CYBERSPACE:

MALEVOLENT ACTORS, CRIMINAL OPPORTUNITIES, AND STRATEGIC COMPETITION

Phil Williams and Dighton Fiddner, EDS.

UNITED STATES ARMY WAR COLLEGE PRESS

Carlisle Barracks, PA

STRENGTH and WISDOM

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

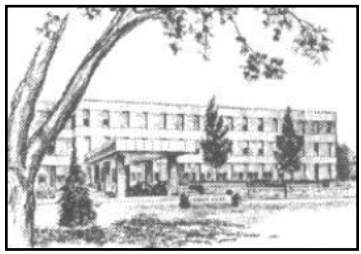
The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

CHAPTER 14

IDENTIFYING THE REAL AND ABSOLUTE ENEMY

Rob van Kranenburg

> But I could imagine, the logical consequence of the Internet of Things is not just a new philosophy of how we can control our production and logistics. It completely changes the paradigms of sequences of operations. . . . The future is not predictable! But we try to predict our future every day. . . . The future will be self-controlled and service-oriented, in other word: the Internet of Things and Services.[1]

TO PREDICT

In his "Wired Opinion, The Internet of Things Has Arrived—And So Have Massive Security Issues," Andrew Rose falls into his own blind spot. It is not an obvious one. In fact, he seems to agree that we cannot predict how things will turn out. He says:

> I am hard-pressed to find a catastrophic scenario associated with the refrigerator—other than the refrigerator spending your entire month's pay on milk or becoming self-aware like Skynet—but the fact remains we can't predict how things will look. That makes regulation and legislation difficult.[2]

This is indeed the thing we humans tend to do: we either underestimate or overestimate. Over a century ago, John Elfreth Watkins, Jr., published "What May Happen in the Next Hundred Years" in *The Ladies Home Journal,* December 1900. His Prediction #4 is not one of his best guesses:

> Prediction #4: There Will Be No Street Cars in Our Large Cities. All hurry traffic will be below or high above ground when brought within city limits. In most cities it will be confined to broad subways or tunnels, well lighted and well ventilated, or to high trestles with "moving-sidewalk" stairways leading to the top. These underground or overhead streets will teem with capacious automobile passenger coaches and freight with cushioned wheels. Subways or trestles will be reserved for express trains. Cities, therefore, will be free from all noises.[3]

Watkins extrapolated from the vision of mobility of trams, trains, and subways, and as a result, could not envision the massive number of cars that would come to congest most cities. Closer to home, in 2001, when interviewed by Charlie Schmidt, then vice president of technology at Automatic Identification and Mobility (AIM), a trade association for manufacturers of tagging radio-frequency identification (RFID) technology, Steve Halliday claimed: "If I talk to companies and ask them if they want to replace the bar code with these tags, the answer can't be anything but yes. It's like giving them the opportunity to rule the world."[4]

All of these thinkers are able to accept massive change at one level while keeping others constant. Halliday is correct to assess the potentially disruptive character of RFID and, by extension Internet of Things (IoT), but could not or would not consider that the Internet, open source software, and open hardware is empowering not only companies he represented or envisaged, but also, a messy field of crowd-funded start-ups. In a similar vein, Andrew Rose stated:

> Given the wide-reaching impact of the IoT, formal legislation and government involvement is almost

> certain. Especially when we consider the safety risks of automated systems interacting in the physical world—governments won't be able to stand by silently if autonomous decisions endanger lives.[5]

In other words, Rose foresees all kinds of risks but insists that government as such will still be able to "ensure" anything. Yet, is this not as realistic as taking the opposite view by arguing that in different ages different agencies over resources defined power, and IoT might represent such a change? If that is the case, there is no longer any government, as we know it.

The discrepancy between what will change and what will remain constant thus seems to be only partly due to discerning data from noise, as it is a recurring issue in all predictions of the future.

BIOLOGICAL AND EVOLUTIONARY CONSTRAINTS TO CHANGE

"DNA ties us all together; we share ancestry with barracuda and bacteria and mushrooms, if you go far enough back."[6] Spencer Wells shows in his Genographic Project through our shared DNA how we are—in all our diversity—truly connected.[7] He argues that it was 10,000 generations or 50,000 years ago (relatively recent in evolutionary terms) that language and non-domain related expression (arts) kick-started toolsets that led to the cultural, social and artistic intricacies that we have today.[8] Before that, the cognitive tools and material toolsets appear to be quite constant over a long period. The difference was made by language acting as a tool for cooperation and negotiating. Both the explosion of variety in practices and tools and many of the crises we confront today have their roots, and he argues, in the dawn of the Neolithic:

> We spent an enormous amount of time as hominids and as primates living as hunter-gatherers. That is the natural way for us to live, and we're suddenly living in this profoundly unnatural way, and we're still in the process of adapting to it and working out how to live with it. . . . We were once used to living in groups of no more than about 150 individuals. Now we live in cities of millions and the cultural cacophony creates a feeling of unease and we are seeing evidence of that with the rise of mental illness.[9]

Wells believes there is hope—what he calls "Pandora's seed." "When Pandora opened the box, she at least had to slap it shut fast enough to contain hope. . . . The hope is that humans are innately innovative and that we can innovate very rapidly when we're forced to." [10]

REAL AND ABSOLUTE ENEMIES

Carl Schmitt distinguishes between *der Wirkliche Feind* and the *Absolute Feind* (the real enemy and the absolute enemy). The latter is "*die eigene Frage als gestalt*" (His own question as shaped). The absolute enemy is the inability to change convictions, alliances, and opinions. The absolute friend is always very near to you, consisting of everyday routine skills; it is your blind spot. The real enemy can differ from time to time and period to period. Each historical situation demands the capabilities to define as those real enemies the ones that can redefine all that you hold normal, dear, and take for granted. It is clear that only rarely do these threats to ontologies, (what you "are," what you hold yourself to "be," what you believe to be "normal," "just," and "fair") lead to classical or asymmetric warfare. One cannot fight depression, weather,

climate change, or religious beliefs, because there is no clear definition of what a victory would mean—other than having things **not** happen. Nor can temporary success be clearly defined. Most important, however, these situations offer no context or markers—openings—to make an informed choice about the kind of weapons that could either be used for defense or offense.

ENERGY

War is about energy, not necessarily about people. In the days of the battle of Culloden Moor, Scotland, arms smashing other arms got tired and gave way. Richard Overy shows in *Countdown to War* (2009) that the decision to go to war in 1939 was made on both sides in a state of "growing irrationality."[11] Protagonists on either side were dead tired. The decision to go to war came as a **relief** to them. By then, the technologies of war had advanced to such an extent that battles could be prolonged potentially indefinitely. Armor tires in a much slower way. Robots do not get weary at all and need no sleep. According to Ronald Arkin, a roboticist at the Georgia Institute of Technology, who is developing ethics software for armed robots by crunching data from drone sensors and military databases, it might be possible to predict, for example, that a strike from a missile could damage a nearby religious building. Clever software might be used to call off attacks as well as initiate them.[12] Still, as long as the machines cannot pay for themselves, it is people who make decisions on who does what kind of fighting and where. Human beings still decide on the nature of war, the definition of a threat, an asset, a risk, and the vital necessities and resources that are

deemed necessary to live. Yet, it is clear that the kind of intelligence that is most apt to make these decisions differs from the times of Culloden; Stalingrad, Russia; and Operation EAGLE CLAW in Iran.

In the age of the battles of men, all was analogue. What you saw is what you got and smelled as you heard the murmurs and sighs of men bleeding to death, with feet, arms, or legs chopped off. There was innovation in tactics, in choosing terrain, in the choice of weapons, but in this space where men were still seeing other men kill or be killed, innovation in the face of unknown outcomes has always followed certain rules and procedures.

When tanks became decisive in World War II, each bloc innovated along its own strengths and weaknesses (German Tiger, Soviet T-34, and Allied Sherman). None of the three blocs invented something significantly different or another mode of fighting. Indeed, all three stayed within conventional thinking and innovation within their own particular sensibilities and cultural schemata under certain specifications and requirements, to be validated in action, immediately enabling rapid feedback and improvement cycles, clear goals and objectives, and a clear win or lose scenario. Unsurprisingly, this situation has become the natural habitat of innovation: companies grow big and compete with each other on details building corporate branding, innovate under specific requirements, validate in real time, immediately enabling rapid feedback and improvement cycles, and demand clear goals and objectives and win or lose scenarios.

After World War II, the entire field of operations was taken to a different level where analogue contexts no longer defined the course of action, policy, and the direction of future investments. The RAND Corpora-

tion took the battlefield to space, thereby introducing and eventually rendering the axiomatic drivers to the digital age of computers and coding.

It was the clear insight of the military commanders and political leadership that the new operational fields would require a new kind of intelligence to lead and co-direct alongside traditional military expertise: the speculative and creative engineer-researcher who was able to define his very own new territory where there was none before. In this context, it was RAND that saw space as a way to harness and direct operational resources anywhere on the planet. RAND was able to embody and direct at the same time a cultural, social, and political shift toward a beginning of evidence-based policy and research and development (R&D), building up datasets that were to be used as input for policymakers. In order to do this, it literally created its own axiomatic borders and playing ground. It therefore built a new ontology alongside the old one of traditional and analogue warfare. This new ontology posed new questions, created new definitions of threat, risk, assets, security, and even the very nature of war. RAND was able to do this because of a balance of disciplines and funding, choice of use cases, and building of new methodologies:

First, was the profound understanding by the military and political leadership of the deep nature of the change that was needed to face the consequences of a reality that had been shaped by the tools of the day. As Commanding General of the Army Air Force, H. H. "Hap" Arnold wrote in a report to the Secretary of War:

> During this war the Army, Army Air Forces, and the Navy have made unprecedented use of scientific and

> industrial resources. The conclusion is inescapable that we have not yet established the balance necessary to insure the continuance of teamwork among the military, other government agencies, industry, and the universities. Scientific planning must be years in advance of the actual research and development work.[13]

Second, was understanding the importance of choosing the right use case, that, in its successful design, showed more than the mastering of certain skills and techniques. In this connection, the emphasis on space was prescient. As the special memoranda abstract summarizing Project RAND working papers and follow on reports noted:

> . . . the most riveting observation, one that deserves an honored place in the Central Premonitions Registry, was made by one of the contributors, Jimmy Lipp, head of Project RAND's Missile Division, in a follow-on paper 9 months later: 'Since mastery of the elements is a reliable index of material progress, the nation which first makes significant achievements in space travel will be acknowledged as the world leader in both military and scientific techniques. To visualize the impact on the world, one can imagine the consternation and admiration that would be felt here if the United States were to discover suddenly that some other nation had already put up a successful satellite.'[14]

Third was a recognition of the need for new methodologies. This was evident in the introduction of the first report of Project RAND, *Preliminary Design of an Experimental World-Circling Spaceship*, released May 2, 1946, from the key passage found on page 4:

> It cannot be emphasized too strongly that the primary contributions of this report are in methods, and not in the specific figures in this design study. One point

> in particular should be highlighted: - the design gross weight, which is of the greatest importance in estimating cost or in comparing any two proposals in this field is the least definitely ascertained single feature in the whole process. . .The most important thing is that a satellite vehicle can be made at all in the present state of the art.[15]

The successful combination of A, B, and C—balance of disciplines and funding, choice of use cases, and building of new methodologies—is rare. When it succeeds, however, it means a period of hegemonic and infrastructural domination, as we have witnessed in the leadership of America until now. Unless the United States is able to repeat this process, it will lose this leadership.

In an American context, it was RAND that managed the transition from Culloden, Antietam, and Stalingrad to space. The transition to robotic warfare, however, has to be negotiated by a network of varied and widely diverging skillsets that allow for conflict **inside** the network.

THE INTERNET AND THE INTERNET OF THINGS

In a future world of super-senses, as Martin Rantzer of Ericsson Foresight has argued, "new communication senses will be needed . . . to enable people to absorb the enormous mass of information with which they are confronted."[16] He also claimed that the user interfaces we use today to transmit information to our brains threaten to create a real bottleneck for new broadband services. Implementing digital connectivity in an analogue environment without a design for all the senses leads to information overload.

In a ubiquitous computing (ubicomp) environment, the new intelligence is extelligence, "knowledge and tools that are outside people's heads."[17]

Against this background, we are currently on the verge of witnessing the emergence of a:

> mega-market, where markets such as home and building automation, electricity generation and distribution, logistics, automotive as well as telecommunication and information technology will steadily converge. We do not know the consequences of connecting all these smart objects (smart meter, e-vehicle, cargo container, fridge etc.) to the Internet.[18]

Professor Michael ten Hompel, Managing Director of the Geschäftsführender Institutsleiter, Fraunhofer-Institut Materialfluss und Logistik (Fraunhofer Institute for Material Flows and Logistics), described the consequences this has for something as "solid" as logistics:

> The logical consequence of the Internet of Things is not just a new philosophy of how we can control our production and logistics. It completely changes the paradigms of conventional supply chain management. Within the Internet of Things the supply chain will be created in real time: *Entities*, consisting of objects and a piece of (agent based) software, generate the resulting supply chain on the move. Therefore the sequences of operations are not predicted. This leads to a new understanding of how to handle our logistic management which won't be a supply chain (!) anymore.[19]

Ten Hompel is not a Science Fiction writer; nor is he is projecting a vision. He is simply describing an emergent reality that, to a large extent, is already here.

It is important to understand that the Internet and the IoT combined change the very nature of power.

Psychologists specialized in the behavior of larger groups of people explain:

> . . . the relative ease with which one is able to exert influence over masses by assuming a causal force which bears on every member of an aggregate, and also for each individual there is a large number of idiosyncratic causes. Now let us suppose that the idiosyncratic forces that we do not understand are four times as large as the systematic forces that we do understand. . . . As the size of the population increases from 1 to 100, the influence of the unknown individual idiosyncratic behaviour decreases from four times as large as the known part to four tenths as large as the known part. As we go to an aggregate of a million, even if we understand only the systematic one-fifth individual behaviour as assumed in the table, the part we do not understand of the aggregate behaviour decreases to less than 1 percent (0.004).[20]

This shows how top-down power works and why **scaling** has become such an important indicator in such a system of "success." Imagine you want to start a project or do something with your friends or neighbors, say five people. This means that you have to take into account before you do anything—state a goal, negotiate deliverables, or even a first date on which to meet for a kick-off—that all five people relate to huge idiosyncrasies and generic forces that have to be aligned or overcome before you can even say hello. This shows how difficult it is to start something. It also explains why you are always urged to get bigger and why you need to grow. It is only then and through the process of getting bigger itself that the management tools can operate, lying in wait for you to discover them. To be decisive, make a difference, to set about a course for change is in no need of growth. Under-

standing the nature of these social relations in these terms shows how difficult it is to script moments of fundamental change, as hierarchical systems by the very fact that they are top down can concentrate on managing systematic forces relatively effortlessly.

With the Internet, however, these idiosyncrasies have been able to organize and raise their weight in the ratio, and the IoT will allow these even further, bringing the sensor network data sets to individuals who can handle them on their devices. This acceleration of weak signals into clusters, organized networks, and flukes cannot be managed anymore by formats that are informed by and that inform systematic forces as the **nature of these forces** have changed.

Thus, it is always difficult for policy to deal with systemic change. It is extremely natural for it to see the above operation as an **attack** on its system and not as a **new iteration** caused by the hegemonic forces it has allowed to operate: education, freedom of speech, consumerism, and the Internet. In nearly all instances, we see revolutions break down in such constellations. It is also understandable that **super-empowered individuals** identified by state and intelligence actors are a major threat to the system (democratic capitalism) as a whole.[21] In the light of the above discussion about the new environment, however, this is not a threat, but an **opportunity**.

In our current architectures, we are used to dealing with three groups of actors: citizens/end users; industry/subject matter experts; and those involved in governance/legal matters. These all are characterized by certain qualities. In our current models and architectures, we build from and with these actors as entities in mind. The data flow of IoT will engender new entities consisting of different qualities taken from the former three groups diminishing the power of the tra-

ditional entities. The IoT will break them. It will force a divorce. This divorce can be brutal or friendly.

If we want to define power to its core, we can say that it is the self-assigned agency of states to assign numbers to people (legal-illegal), and the self-assigned agency of companies to isolate data in Internet Protocol and copyright and patents (legal-illegal). They are wed together. Without the former, the latter has no capability to enforce any laws. Without the second, the first has no capacity to ensure that citizens do not start to question why they should keep paying taxes, as some level of convenience is provided.

The Internet brought this wedding into question as the only possibility to posit as a foundation for everyday life and praxis. It revealed how much legacy is actually still in this combination built on violence, isolation of data, and (preferably phrased as "healthy") competition. A quick look at the top 100 companies before and after the Internet shows how disruptive the Internet is.

IoT means full traceability, and not one thing is unmonitored or out of sight. All and everyone are in full light. There will be no more users who need to secure privacy, as the concept of privacy has to be distributed over the qualities of the new actors. There will be cookies on the table you put your cup on, and, no, you do not want to be notified how long this table will store the information that you had an espresso there.

It enables new forms of work, redefining what a "job" is:

> By 2020, more than 40% of the U.S. workforce will be so-called contingent workers, according to a study conducted by software company Intuit in 2010. That is more than 60 million people. We are quickly becoming a nation of permanent freelancers and temps.[22]

Strangely:

> the Americans in their 20s and 30s who will be most affected by it remain decidedly upbeat. They are much more hopeful than older generations, polls show, that the country's future will be better than its past. Based on what younger adults have been through, that resilience is impressive. It's probably necessary, too. The jobs slump will not end without a large dose of optimism.[23]

All this is possible because of the monitoring capabilities that are embedded in these practices that enable business-to-business (B2B) and customer-to-customer (C2C) without third party costs on liability or accountability.

Another kind of service could consist of offering real-time threat analyses, showing that the threat of a terrorist attack for individuals is 0.0001 percent and, for the sake of argument, slipping and falling in the bathroom is 0.3 percent.[24] At an airport where people use Layar, Google Glasses, Twitter, and LinkedIn—and where nobody wants to be blown up—the worst thing that can happen is that erroneous information about fellow passengers is obtained from the accessible databases. In such an environment, more and more fatal misunderstandings can occur. Umar Farouk Abdulmutallab slipped through the net of the regular security dashboards. If we were to feel once again responsible for our own actions and safety, perhaps we would have intercepted him earlier.

In this new **conceptual** space, we have to build new notions of privacy, security, assets, risks, and threats tailored to a reality of today, not a reality of yesterday or further back in time. So our main question now is to

stare reality in the face and tell civil society and competing military doctrines to stop fighting lost causes from intrinsically untenable and un-fortifiable positions. To start a methodology that allows us to identify a number of real enemies and the absolute enemy that the U.S. military, and by definition, the United States (as the military takes about half of every tax dollar of citizens) is facing. It comes down to deciding when it is time to act out of a deep knowledge that the current situation is untenable. Unfortunately, the analysis of the situation leaves different stakeholders with different timeframes. Nevertheless, there are ways forward.

In his seminal text, *The Social Order of a Frontier Community*, Don Harrison Doyle wrote, "social conflict was normal, it was inevitable, and it was a format for community decision making."[25] Sociologist Lewis Coser also advised that, instead of viewing conflict as a disruptive event signifying disorganization:

> We should appreciate it as a positive process by which members of a community ally with one another, identify common values and interests, and organize to contest power with competing groups.[26]

The new environment of the IoT will resemble these "frontier communities" because of their seeming disorganization where conflict will be the norm.

We are in need of a new iteration of a successful combination of A, B, and C, a balance of disciplines and funding, choice of use cases, and building of new methodologies. It is difficult, but whoever succeeds will enter a new period of hegemonic and infrastructural domination. A means negotiating real and absolute enemies with new stakeholders such as the open source community, the WikiLeaks Crew, and Anonymous Hackers, Bradley Manning, the activists of Open

Hardware, Software, Innovation, and Data. For B, the use cases must be novel, real, and testify to the creation of new kinds of knowledge of material processes. When Steve Jobs returned to Apple in 1997, one of the first things he did was close down the Advanced Research Group, saying research needs to be done in the crucible of development. Low hanging fruit for us in 2015 are, sewage systems, bridges, roads, and inner city development, in short taking the space metaphor back to Earth in a **smart**, **hybrid** way. C is about creating spaces for new definitions about what is data and what is noise that underpins new temporary forms of reading and outputting new combinations of sensor, visual, and text data.

Stated more baldly, it is clear as Global Futures Partnership noted:

> The increasing globalization of R&D, real-time diffusion of technical knowledge through international networks, and the convergence of advancing technologies are creating new challenges for global security. Innovations in such diverse areas as ICT, biological sciences, neuroscience, material sciences, nanotechnology, and robotics could provide hostile actors increasingly cheap access to a wide range of technologies. Destructive application potential of rapidly advancing innovations is compounded when the technological convergence is considered. Emerging and commercially available technologies can be used in novel and undesirable ways to achieve political, military, or monetary goals.

To meet this challenge, we just need a commanding general like Arnold to stare reality in the face and tell civil society and competing military doctrines to stop fighting lost causes from intrinsically untenable and unsustainable positions. To develop and implement

a methodology that facilitates the identification of a number of real enemies as well as the absolute enemy that the U.S. military and by definition the United States (as the military takes about half of every tax dollar of citizens) is facing. It is important to move ahead rapidly and decisively.

ENDNOTES - CHAPTER 14

1. Personal mail to the author by Professor Dr. Michael ten Hompel, who holds the Chair of Materials Handling and Warehousing at TU Dortmund University and is managing director at Fraunhofer-Institute of Material Flow and Logistics (IML).

2. Andrew Rose, "The Internet of Things Has Arrived—And So Have Massive Security Issues," Wired, January, 11, 2013, available from *wired.com/2013/01/securing-the-internet-of-things/*.

3. John Elfreth Watkins, Jr., "What May Happen in the Next Hundred Years," *The Ladies Home Journal*, December 1900, available from *yorktownhistory.org/wp-content/archives/homepages/1900_predictions.htm*.

4. Charlie Schmidt, "Beyond the Bar Code," *MIT Technology Review*, March 1, 2001, available from *technologyreview.com/featuredstory/400913/beyond-the-bar-code/*.

5. Rose.

6. Spencer Wells, "A family tree for humanity," TEDGlobal 2007, June 2007, available from *ted.com/talks/spencer_wells_is_building_a_family_tree_for_all_humanity*.

7. Spencer Wells, *The Journey of Man: A Genetic Odyssey*, Princeton, NJ: Princeton University Press, 2002; and New York: Random House, 2004, p. 75.

8. Wells, "A family tree for humanity."

9. *Ibid*.

10. Spencer Wells, *Pandora's Seed: The Unforeseen Cost of Civilization*, New York: Random House, 2010.

11. Richard Overy, *1939: Countdown to War*, New York: Viking, 2009.

12. "March of the Robots," *The Economist*, Technology Quarterly, 2nd Quarter Ed., June 2, 2012, available from *economist.com/node/21556103*.

13. *A brief history of RAND*, Santa Monica, CA: RAND, available from *rand.org/about/history/a-brief-history-of-rand.html*.

14. RAND, Special Memoranda, website abstract for the reports pertaining to Project RAND, available from *rand.org/pubs/special_memoranda/SM11827.html.*

15. *Preliminary Design of an Experimental World-Circling Spaceship,* Santa Monica, CA: RAND Corporation, 1946, available from *rand.org/content/dam/rand/pubs/special_memoranda/2006/SM11827part1.pdf,* p. 4.

16. Martin Rantzer, *Foresight Paper – All Senses Communication*, No. ERA/SVZ/R-01:029 Uen, Ericsson, 2001.

17. Ian Stewart and Jack Cohen, *Figments of Reality*, Cambridge, UK: Cambridge University Press, 1997.

18. Jens Strüker (*strueker@iig.uni-freiburg.de*) *et al*., on the LinkedIn Group, "Internet of Things," 2011.

19. Personal mail to the author by Professor Dr. Michael ten Hompel.

20. Arthur L. Stinchcombe, *Constructing Social Theories*, London, UK: The University of Chicago Press Books, 1968, pp. 67-68.

21. Rob van Kranenburg, "Transformational Technologies #4: Implications for an Expanding Threat Environment," presentation at workshop "Transformational Technologies: Implications for Global Security," Rome, Italy, September 17-18, 2012.

> This Global Futures Forum workshop is the fourth in a series titled 'Transformational Technologies: Implications for Global Security.' On behalf of the Global Futures Forum community, and in partnership with the Italian Intelligence Community, it is our honor to host this GFF workshop at Palazzo Salviati, Headquarters of Centro Alti Studi Difesa. All remarks will be unclassified, off the record, and not for attribution.

"If the pace of technology continues at this rate, greater technological change will occur in the next 20 years than has occurred in the whole of the 20th century. . . ." The Lipmann Report Eds., "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk," *Foreign Affairs Magazine*, The Lippmann Report, November/December 2010.

22. Jeremy, Neuner, "40% of America's workforce will be freelancers by 2020," *Quarz*, March 20, 2013, available from *qz.com/65279/40-of-americas-workforce-will-be-freelancers-by-2020/*.

23. David Leonhardt, "The Idled Young Americans," *The New York Times*, May 3 2013, available from *nytimes.com/2013/05/05/sunday-review/the-idled-young-americans.html*.

24. *Preliminary Design of an Experimental World-Circling Spaceship,* p. 4. "It cannot be emphasized too strongly that the primary contributions of this report are in methods, and not in the specific figures in this design study."

25. Don Harrison Doyle, *The Social Order of a Frontier Community: Jacksonville, Illinois, 1825-70*, Urbana, IL: The University of Illinois Press, 1983.

26. Lewis A. Coser, "Social Conflict and the Theory of Social Change," *The British Journal of Sociology*, Vol. 8, No. 3, September 1957, pp. 197-207, available from *jstor.org/stable/586859*.