What we call the “information environment” increasingly describes the entire geo-strategic environment. There is no distinct informational domain, as there is a domain of land or sea or even cyber. Rather, “information” is the global air we all breathe. If this is the case, what are the implications for developing, and execute strategies and tactics related specifically to information?

By Amy Zalman, Ph.D.

Presented to the visiting delegation of the Swedish Defence College, U.S. National War College, Washington DC

October 21, 2013
Information is the global air we all breathe

Good morning. The topic of this talk is National Strategy in a Maturing Information Age. Its broad premise is that what we call the information environment increasingly, actually, describes the entire geo-strategic environment. That is, there is no distinct informational domain, as there is a domain of land or sea or even cyber. Rather, information is the global air we all breathe. If this is the case, what are the implications for those of us who theorize, develop, and execute strategies and tactics related specifically to information?

Later today and over the course of this week, you will hear from speakers about operational information operations, that is—the specific science and art of shaping the perceptions of key stakeholders in the context of military activity. You will also have much opportunity to discuss the cyber domain, and international efforts to define and establish norms within it. You will learn how the Department of Homeland Security seeks to protect cyber and communications assets, how our new Cyber Command is coming along, and about the current relationship between intelligence and strategic communication.

As the first speaker in your series, I am going to start in a different place, the broader context within which those activities fit. At the National War College, where I teach, our officers are instructed according to a construct we call DIME, in which the instruments of national power are divided into Diplomatic, Informational, Military and Economic. As military professionals whose entire objective here is to investigate “information” in military contexts, you will immediately see some of the internal contradictions of that division between military and informational tools of power—which is part of what I intend to address.

We further suggest that military strategy, in combination with the other three elements of power—informational, diplomatic, economic—together supply all of the ingredients required to fulfill a national strategic objective, which supersedes military strategy in itself.

The locus of my talk is this latter, “higher” space, where national strategic objectives are conceived and fulfilled, and where international allies join in coalitions and partnerships to produce supranational ends.

The point of speaking from this space is not to diminish the operational aspects of information and influence capabilities. Indeed, it is exactly the opposite. I want to talk with you about how the geo-strategic environment is changing, and why the expertise and assumptions that
are the daily bread of the information operations community are so necessary to understanding this changing world.

This is the Information Age—also known as the age of cyber, the digital era, the era of networks. The information revolution, like the industrial revolution before it, is both global and total, in the sense that it does not simply describe the processes of economic production, nor changes in commercial transactions and how we organize economic activity, but changes in how we relate to each other as humans in every sphere or our activity.

This does not mean that what we know about ourselves now is irrelevant, nor that our inherited understanding of the nature of strategy and war will fall by the wayside.

Rather, we are a species whose behavior always carries the imprint of our history. Human behavior in the present generally tells the story of a negotiation between our inherited, historical self and the unknown future.

We are in that negotiation right now. In 2008, then Secretary of Defense Robert Gates wrote a memo on the topic of Strategic Communication and Information Operations in the Department of Defense. He began like this:

“The United States finds itself in the midst of a rapidly changing strategic environment. The erosion of traditional boundaries between foreign and domestic, civilian and combatant, state and non-state actors and war and peace is but one indication of this change. Today, geographic borders have diminished in importance as non-state actors have increased their role in globally-diffuse terrorist networks and transnational activity.”

Gates’ statement is no longer news to us. We could all probably throw out similar rhetoric in our sleep at this point. But we should probably resist becoming complacent about it, because the effect of the changes embedded in that statement will ultimately reach the bedrock assumptions of our international system, the system of sovereign nation-states seeking a balance of power, and shake them up in a very big way. We are just seeing fault lines now, and these are the products of the information revolution — of the advance in digital technology and now in technological convergence.
In his 2008 memo, Gates goes on: “In response [to these changes], the President has heightened U.S. Government strategy emphasis on countering violent extremism through effective strategic communication (SC) and information operations.”

Which is to say, that at an early point in our understanding of the changes that the information age has produced, the US government sought to employ the informational arts to address them. This was a prescient moment.

And the reason it was so visionary was because it matched so precisely the logic that governs strategic threats in the information age with a solution that shares that same logic. This is, perhaps, a slightly different way of saying, and paying homage to John Arquilla and David Ronfeldt’s insight in the 1990s that it “takes a network to fight a network.”

Let us explore this idea further through the example violent extremism, as an exemplary form of 21st century threat.

**Violent extremism is a problem rooted in human perception and psychology, extended by networked social relationships, and complicated by feedback loops, which are enabled by digital technology, that compound kinetic effects with communicative ones.**

Think of the global circulation of the images of the falling World Trade Center in 2001, which made the global media an unwitting handmaiden of terrorism, which relies on the imagery of terror to create its effects.

Or the case of Anders Breivik, who as you know, was motivated by a complicated ideological cocktail of Islamophobia, anti-feminism and a self-styled version of Zionism, when he murdered 77 people in Oslo several years ago. Feedback loops in networked conditions produce truly unpredictable results—and that is what Breivik was.

Let me be clear. I am not talking about addressing 21st century’s most complex issues with information tactics. This is not about papering the complexities of the information age with leaflets, or tweets. It is about beginning to peer into the unfolding logic of our own age to understand better its threats, and exploit far more effectively its many positive opportunities.
The logic of our age: What is, then, that logic? I will talk with you about three of its forms—the logic of networks, the communicative logic of power, and the fact of multi-stakeholder governance.

First, it is the logic of networks. We need to learn to see and feel what that means. So here is a visual analogy based on my extremely recently gained knowledge of that favored Swedish sport, Bandy. Bandy, as I understand it is something like European football, which we call soccer, played on ice.

One form of strategic vantage in Bandy is from the point of view of a player, facing down the opposing team and trying to see their way to a goal. A second is from the stand, where the cheering crowds are of course rooting for Sweden, and definitely not for Finland. And apparently also drinking regularly from the flask they keep in their “bandy briefcase.” But the only figures on the field or rink are the players, and possibly other stakeholders, such as referees. This vision assumes binary opposition of two teams, as well as the ability to find a place off the field to watch the action. It presumes that people are organized according to their participation in particular groups.

Networks are different. Imagine that everyone in the scenario above, players, bystanders and all, has a device that enables them to connect in real time with anyone else either in the stadium or beyond.

Do you have that? That’s good, because we now have to abandon the analogy. And move to irregular war. The logic of irregular war, insurgency, terrorism, tells us that there is no stadium, no delimited battlefield.

Players—that is, combatants—can be anywhere; victims can be anywhere. This was the lesson of the late 20th century. The Popular Front for the Liberation of Palestine could hijack an American plane leaving Rome to publicize globally its strategic aims. And be on the nightly news, and in the news the next morning.

But the 21st century takes us one step further, which is the de-territorialization and de-temporalization of conflict. The 9/11 attacks took place in New York City and Washington. But they also took place, as it happened, in Oslo. And they last as long as their recording in digital form, which is to say, forever. And in combination with other unfolding events, they eventually produced Anders Breivik.
There is much to say about networks, both human and digital, and in their interaction. Just a few points.

First, networks do not have an outside. There is no position outside the action. This is important for Americans, in my view, because institutionally we have the tendency to take ourselves out of our representations of feedback loops. We project, but forget we are also being projected on. To take an example: In 2010, the research organization International Council on Security and Development (ICOS) interviewed 1500 men in Helmand and Kandahar in southern Afghanistan. 92% were unfamiliar with the events of 9/11. They consequently had no idea why the Americans or Coalition troops were in Afghanistan.

One way to read this situation is to say, wow, this is really a backward place. Those Afghans are completely disconnected from the global media! But another way to read it is that being outside of that media, and having nothing to do with those events did not prevent them from becoming part of their unfolding effects. The playing field, in a networked world, is anywhere and everywhere.

The more salient item I want to highlight is about recognizing oneself as inextricably part of networked events. Another way to read this situation is to look at the Americans, as reacting to an event in the network—in the global network of political and politicized actors—in a way that produced unintended consequences.

There is no outside to the network. So we have to learn to look at the field both from the player’s prospective and in a rendition of the whole that includes us.

Second, on networks, we need to continue to understand the interaction between we humans and our information technologies. This is especially the case as we move into an era in which a truly mind-boggling number of tools we use become conduits for information in digital, and therefore aggregable, form. To date, these two discourses—people and technology—are often held at bay from each other in operational and policy environments. So there are discussions of the technologies themselves, and how to protect and exploit them. And there are various discussions about the institutional behavior around them, but there is less discussion about the potentially strategic effects of new behaviors by citizens, non-governmental organizations, private firms and governments in this evolving environment.
The discussion that does exist can be on the hyperbolic side — tending either toward hyper-techno-optimism, of the sort that Google CEO and former State Department official Jared Cohen display in their new book, The New Digital Age, or pessimism, which is less hyper, such as Yvegeny Morozov.

What we need is the “just-right” analysis of the sort that information operations’ professionals are used to — how are people likely to engage with information technology? How could we? What forms of new behavior, for example, is the increasing network convergence producing?

And, although it has been noted that the greatest cyber vulnerability we have is ourselves, it bears repeating. And repeating. The term that information security professionals use to describe psychological manipulation is “social engineering.”

Jordan Harbinger, who recently performed an experiment to see whether he could insinuate himself into companies that classified work calls it “human hacking.” By day, he is actually a dating coach—that is, he knows all about how men and women play tricks on, and seduce each other. In his experiment, he started at LinkedIn, which as many of you know is a professional networking website, which actually groups on it for people with security clearances.

He created a false identity, as an engineer, and joined one of these groups. He then created a second false identity as a recruiter, and sent out false messages calling for job applicants. Although he was vague about the opportunity, respondents trusted him because he was in a top-secret clearance group. He used the small bits of information that the mostly male, mostly engineering group to do further research on them, learning through their other social media sites where, for example, they liked to have coffee and work.

At a place like Starbucks, with its open network, he could gain entry to their network and then he could do serious snooping. The piece de resistance of his infiltration campaign was to create one final cover—a Facebook profile of an attractive female college student about to graduate with an engineering degree. Under cover of this student, Harbinger went to some of his targeted engineers with a note about how she had received an offer from their company, but wasn’t sure she wanted to work there, and asking if they liked their projects. As Harbinger told an interviewer for National Public Radio about his experiment:
“Guys love to come to the rescue, so I played that vulnerability. Damsel in distress. I’m looking for a job, I don’t know what to do, can you help me? A lot of guys were like, I’m not supposed to tell you this, but I’m working on this. It is so cool; it’s got billions of dollars in funding.”

The moral of this story, as Harbinger himself pointed out, is that companies will commit tremendous resources to technical defenses, they don’t necessarily train employees. In brief, the networks that we need to keep our eyes on are human ones, as Information Operations professionals have always known.

So, the first element of the logic of the information age is that it is the logic of networks.

A second crucial element of the logic of our era relates the character of power. Power is the capacity to get things done, it is an inchoate quality until it finds expression in different tools or channels.

Power in the context of geopolitical and military strategy has for many centuries referred to the capacity to wage and win wars, because war was the route to the survival and aggrandizement of the state. The informational battle—for the hearts and wills of men—has always been an element of that capacity, as strategists throughout history have recognized. But it was always subsidiary to superior capacity for organized violence as the ultimate arbiter of power.

In the early 1990s, political theorist Joseph Nye coined the idea of soft power, which he described as the co-optive power of attraction, rather than the coercive power of armed force. He developed this idea at a moment when many in the U.S. Policy community feared the country was declining in traditional command power. This was very good news, for it told us that not only were we still powerful, we were even more powerful than we might have previously imagined. On the other hand, it was bad news, in my view, for theorists the world over have now spent over 20 years arguing over where hard power ends and soft power begins, forgetting that these are not actual phenomena of the natural world, but imaginative constructs with no physical counterpart in the world of things.

The argument masks the more potent insight that in our era, the kind of power he gave name to is more predominant than it was in the past. Variants of coercive force and influence activities have always been elements of power. But different eras define power in distinct ways that stem from their technological capabilities and intellectual tendencies. Two centuries
ago, power was access to raw materials and the ability to control their distribution. In contrast, political and economic power is now largely based on information and information technologies, and globalization of commerce and media they underwrite.

In such conditions, being powerful—being able to produce favorable outcomes in the international arena—requires capabilities that more frequently fall on the persuasive/attractive end of the spectrum. This does not mean that the utility of coercive force entirely fades away, just as it would be misleading to claim that cultural attractiveness, and a favorable image, are entirely new aspects of national power.

Indeed, we are now at a point beyond hard and soft, and we need to recognize this vestigial schematic as more confusing than useful at this point.

Power is now both. Both hard and soft. There is such a thing as the coercive use of influence. And even violent force, or so-called ‘hard power,’ must be considered in terms of symbolic effects and perceptions, these days, because both event and its effects can be more easily recorded and disseminated far and fast from their source.

The point about how to label power is not simply semantic. Categories are the conceptual equivalent of labeled storage boxes: what we call the category tells us what is inside the box. Categories usefully organize concepts for us, but in creating order, they also limit our ability to see new connections between ideas. As long as defense and economic diplomacy remain in a box labeled “hard power,” we fail to see how much their success relies on their symbolic effects as well as their material ones. As long as diplomatic and cultural efforts are stored in a box marked “soft power,” we fail to see the ways in which they can be used in service of coercion or produce effects that are like those produced by violence.

Information Operations— as a military activity dedicated to understanding the communicative effects of instrumental action—is in a supreme position to help other areas of government grasp the nuances of power that is both hard and soft, coercive and symbolic.

In addition to the logic of networks, and the logic of power that is both instrumental and communicative, there will be a third logic of our age. It is nascent yet, and still emergent, but we will soon see that governance and conflict are a multi-stakeholder activity.
Indeed, there is much consideration of this fact already in the kinds of contexts in which we travel. Cyber norms will inevitably engage the private sector, at the institutional level, and all of us everyday citizens, at the level of cyber “hygiene.” The concept of “softwar” developed by one of your speakers of later this week, Chuck de Caro, involves conflict carried out over global television and as you can imagine would engage states, commercial entities, non-state combatants, and citizens. American strategic documents are also forthright about the way in which the landscape has changed, as our QDDR in 2010 observed, it features “an increasingly varied set of actors who influence international debates: more states capable of acting on their own diplomatic agenda, a variety of U.S. Government agencies operating abroad, transnational networks, corporations, foundations, non-governmental organizations, religious groups and citizens themselves.”

But it is fair to say that that real potential implications of this multi-stakeholder world for sovereignty and governance have not yet been considered. In our curriculum at the National War College, these insights do not penetrate a curriculum still dedicated to the premise that the future of governance and conflict is between states.

I would be happy to talk more about this — I gave a talk on this topic alone at the Pentagon last week – but in the interests of time, won’t discuss it more now.

I will simply ask a few questions in brief: what are the legal frameworks that might govern a world in which there are a wide variety of actors? What are its norms, and how will enforcement and performance be exercised? Here is a really difficult one, how will we deal with bad guys who begin to govern - one of my colleagues here at NDU, Michael Miklaucic at the Center for Complex Operations, is concerned about what he calls “criminal states” that are so deeply infiltrated by criminal elements that they are no longer the same kinds of states that we have. But they nevertheless may be “doing governance” for some citizens. Can we simply excise them from the international system? Will normal diplomatic means be enough to work with them to change?

Concluding Remarks

Let me move into a few brief, concluding remarks. I do not think I can offer you solutions, since I’m not offering up a “problem” that needs solving, but rather a changing set of conditions for which particular ways of thinking will be required.
These ways of thinking and understanding already exist in the information and communications community.

They revolve around the recognition that human perceptions, emotions and cognition are at the root of both conflict and problem solving, that culture and history inform the way we behave in the world. They recognize that conflict and its resolution take many forms and that armed force may be the least of them. I was speaking to a colleague who has been in the Information Operations community the other day who is stationed at Fort Bragg, in North Carolina, and he said to me, “It’s much easier to kill someone than to talk with them. It takes me five or six hours to get a CONOPS to approved for armed force, but to get a phone call approved can take five or six weeks.”

Information operators are early adaptors of 21st century logic — the logic of networks, the recognition that all expressions of power have a communicative element and multiple orders of effect, the understanding that many actors are at play and social environments are complex. And they are early to the recognition that “cyber” is not something that takes place in some far off classified space—although it does that too—but in our daily experience, where it is increasingly viewed as a global civil right. Probably one of the few things that the U.S. State Department and the cyber-activists Anonymous agree.

Information operators know about the importance of strategic narrative and of the human tendency to make sense of the world through stories. They are therefore well placed to help political leadership make sense of a world in which complex problems are shared by many stakeholders of various sorts — think of issues such as climate change, poverty, political instability in regional settings —and which require strong stories that will bind these disparate actors to a shared goal.

So, as you go through this week, thinking and meeting with new colleagues who focus on information operations, I invite you to recognize that the operational skills you already have and will continue to deepen are extremely important at this present moment, and that you have much to offer political leadership in understanding our era.

One final note. I also invite you to think about opportunity as well as threat as you go through this week. The French Revolution created a new public sphere, as we know, in which citizens have a voice. The information revolution will take this a step further, and citizens globally are about to have a much greater political influence than they once did.
Militaries typically do not fully trust citizens — who they tend to encounter as victims who need their help or as potential adversaries. Yet the psychology of influence, which is at the core of our work, tells us that humans are predisposed to be generous in their assumptions about others, and trusting to a fault.

When we are not empowered with knowledge and critical thinking skills, we are vulnerable to exploitation, radicalization, and generally bad ideas. But when we are, we are a great force for good, and there are many opportunities for this kind of partnership, as well as the already strong one between NDU and the Swedish Defence College.