

**Shared Knowledge, Joint Pursuits: International Relations Beyond the
Age of Information**

Christopher Pallaris
International Relations and Security Network, Zurich

and

Sean S. Costigan
International Relations and Security Network, Zurich and
The New School, New York

International Affairs Working Paper 2007-02
March 2007

Paper prepared for the annual meetings of the International Studies Association, Chicago,
March 2007

Copyright 2007 by Christopher Pallaris and Sean Costigan

Shared Knowledge, Joint Pursuits: International Relations Beyond the Age of Information

Christopher Pallaris
International Relations and Security Network, Zurich
pallaris@sipo.gess.ethz.ch
www.isn.ethz.ch

and

Sean S. Costigan
International Relations and Security Network, Zurich and
Graduate Program in International Affairs
The New School, New York
costigan@sipo.gess.ethz.ch
www.isn.ethz.ch
www.gpia.info

International Affairs Working Paper 2007-02
March 2007

ABSTRACT

This paper offers an initial attempt to examine international relations (IR) in light of the ongoing information revolution and recent developments in knowledge sharing and educational instruction. Chiefly, it argues for a greater appreciation of the way in which knowledge and learning are shaping the security agenda and the course of international affairs. It urges the IR and security community to make greater use of open learning environments and open source methodologies as a means of knowledge creation, acquisition and delivery. Finally, it advocates the teaching and cultivation of new skills for individuals working in international affairs.

Shared Knowledge, Joint Pursuits: International Relations Beyond the Age of Information

Christopher Pallaris and Sean S. Costigan

This paper offers an initial attempt to examine international relations¹ (IR) in light of the ongoing information revolution and recent developments in knowledge sharing and educational instruction. Chiefly, it argues for a greater appreciation of the way in which *knowledge* and *learning* are shaping the security agenda and the course of international affairs. It urges the IR and security community² to make greater use of open learning environments and open source methodologies as a means of knowledge creation, acquisition and delivery. And it advocates the teaching and cultivation of new skills for individuals working in international affairs. The paper is not the result of a formal research program. Rather, it is largely based on the authors' readings, observations, and discussions with IR scholars and members of the security policy community over the past two years.

≈

For much of the past two decades, researchers working in IR and security studies have sought to understand what impact the information revolution would have on the behavior of state and non-state actors and the conduct of strategy and military affairs. Information, they concluded, was the coin of the realm³, the key determinant of power and authority. The more you had, the more powerful you would be. Information technology, meanwhile, was going to be the most important power resource of the 21st century.⁴ Properly leveraged, it would enable the existing state system to respond more effectively to non-state threats.

This was the decade of “infoprefixation”, of defining old concepts in the light of the information revolution. Researchers on both sides of the Atlantic spoke of information strategy, information warfare, information dominance and information superiority – all of which were to fuel a revolution in military affairs (RMA) that would guarantee the primacy of the West in general and the United States in particular.

Granted, the West's adversaries would try to duplicate these abilities but they would forever be playing catch-up. First movers would hold the best cards; and while the barriers to entry would be lowered, the revolution itself would not lead to the

¹ “International Relations” is used here as the preferred term for the study of global politics and international affairs.

² By “IR and security community” we refer to scholars, researchers, policymakers and practitioners active in international relations and security debates.

³ The term is borrowed from Joseph S. Nye, Jr. and William A. Owens, America's Information Edge, *Foreign Affairs*, Vol. 75, No. 2, March/April 1996.

⁴ Robert O. Keohane and Joseph S. Nye, Jr., Power and Interdependence in the Information Age, *Foreign Affairs*, Vol. 77, No. 5, September/October 1998, p.87.

decentralization of power or the equalization of states. On the contrary, it would have the opposite effect.⁵ This, in turn, would result in asymmetric conflict; lacking the technological advantages enjoyed by the West, its enemies would seek to exploit other weaknesses. But no matter: a closer reading of Sun Tzu, a deeper knowledge of one's enemies, and all would be well.

Elsewhere, the security policy community sought technological solutions to alleviate the consequences of the information age, chief of which was the explosion in the number of open and clandestine information sources and a growing need to share information within and between government agencies. Technology, it was assumed, would provide the silver bullet. Western intelligence agencies spent billions of dollars establishing information infrastructures that would enable vastly improved information collection, storage, analysis, retrieval and distribution. The more information you could get your hands on, the thinking went, the greater your ability to understand and respond to the intentions of your adversary.

The investment seemed justified in light of the dizzying pace of the IT revolution of the 1990s. Intelligence agencies everywhere, but particularly in the West, were grappling with a rising demand for information and greatly reduced operational cycles – due in part to the “CNN effect”⁶. The promises of information technology were too tempting to ignore.

From Theory to Implementation

In any event, these ideas were not without merit. Tested in the crucible of war, some even proved their practical application. The US-led invasion of Iraq in 2003 was a stunning demonstration of how information technology and the RMA can be applied to conventional warfare. It was the culmination of a long process of thought and change in military technique that appeared to vindicate its proponents. The invasion and occupation of Iraq at the cost of 161 dead coalition troops, made the German blitzkrieg appear positively incompetent by comparison⁷. As Andrew Bacevich put it, “these seemingly disparate ideas suggested the onset of a historical era characterized by unprecedented transparency and connectivity. Mankind had embarked upon an age in which technology promised very rapid change, while also bringing total mastery of the human environment more closely within reach. In all sorts of enterprises, technology held the key to power and the United States was indisputably the technologically most advanced nation on the planet.”⁸

The prelude to Iraq even hinted at the capabilities of the US and British intelligence communities to uncover all manner of nefarious activities. Doubtless, some of this was

⁵ Ibid p.89.

⁶ The Brookings Institution ran a debate on the CNN Effect that detailed a number of assertions that 24 hour news coverage have forced the hand of policy makers, including the critical decision to fight the first Gulf War. The text of the debate can be found here: <http://www.brook.edu/comm/transcripts/20020123.htm>.

⁷ Max Boot, *The New American Way of War*, *Foreign Affairs*, July/August 2003, p.44.

⁸ Andrew Bacevich, *The New American Militarism*, Oxford, 2005, p. 169.

true. But closer scrutiny over time revealed gross inaccuracies and accusations of fraud, falsification and worse.

But the post-9/11 and post-Iraq reality now appears very different from what was anticipated in the early and mid-1990s. The promises of the information revolution and RMA would appear to have come undone in an Iraq riven by terrorist violence, civil strife and insurgent warfare.

Elsewhere, the investigation into the “intelligence failures” of 9/11 revealed that there was no shortage of information hinting at an attack on domestic targets. This information had been stored in separate silos and was waiting to be processed and synthesized into actionable intelligence. However, the connections were not made in time. Despite all the investment in IT, the warnings of a previous generation of intelligence analysts proved prescient: there can never be a time when the thoughtful man can be supplanted by the intelligent device supreme.⁹

And yet, the search for the silver bullet continued. Researchers at the Defense Advanced Research Projects Agency (DARPA), for example, were involved in two highly contentious information technology projects: FutureMAP and Total Information Awareness (TIA). FutureMAP was conceived of as a marketplace for speculating on the political developments in the Middle East, including the likelihood of terrorist attacks. The project was cancelled in July of 2003 under pressure from Congress and public outrage at the prospect of terrorists “betting” on their future activities. Total Information Awareness changed its name to Terrorism Information Awareness and encompassed an ambitious and controversial effort once led by Admiral (ret) John Poindexter to create a massive database, populated with a wide variety of information on individuals and their transactions, to help capture the information signature of potential terrorists. TIA was terminated in 2003, this time over concerns of public privacy,¹⁰ although some of the software and designs developed for it live on at the NSA.¹¹

Technology has now proven to be as much a blessing as a curse. While it has certainly helped intelligence agencies to identify, monitor and respond to emerging threats, it has had a negligible effect in countering the ideology of Islamic fundamentalists or stunting the growth of organized crime. If anything, the Internet and word processor constitute some of the most effective instruments in the asymmetric toolbox.

Indeed, rather than serve as a means to an end, technology is increasingly relied on as an end in itself. The tendency within the US intelligence community is to try and solve analytical problems with technical solutions.¹² But the problems remain. The more information you aggregate, the more difficult it is to make sense of it all. Analysis – the process by which information is turned into knowledge - quickly becomes the bottleneck

⁹ Sherman Kent, *Strategic Directions for American World Policy*, Preface to 1965 edition, p.xvii.

¹⁰ As former DARPA Director Charles Herzfeld noted in 1975, "When we fail, we fail big."

¹¹ Shane Harris and Tim Naftali, Tinker Tailor Miner Spy, 2 January 2006, *Slate*, <http://www.slate.com/id/2133564/>.

¹² George Friedman, *America's Secret War*, Abacus, 2004, p.72.

of intelligence.¹³ And it's only going to get worse. With the world's information growing at the rate of 66 percent a year, we have a long way to go before we can begin to make sense of it all.¹⁴

Knowledge: The Key to the Kingdom

So where did the IR and security communities go wrong? Given the time and energy spent on defining the information revolution and forecasting its consequences, why did they fail to anticipate the challenges we face today?

In part, the answer lies in a failure to anticipate or appreciate how a *revolution* in information technology would result in a fundamental *transformation* in knowledge and learning, especially among the West's adversaries. For all the talk of power, few bothered to recall the role of knowledge in the equation. Fewer still would have foreseen how the information revolution would result in the democratization of knowledge or the rapid proliferation of learning opportunities for the common man. In the 21st century, information would be the coin of the realm, but knowledge would prove to be the key.

To be fair, such foresight may not have been possible back in the 1990s. Who could have foreseen the Internet phenomenon or the likelihood of free international phone calls? Who would have anticipated the shift of media power to blogosphere or imagined its adherents as 21st century pamphleteers? Predictions are easy to make and easier to dismiss, especially if they smack of historical or technological determinism.

In any event, IR specialists have a proven track record at not being particularly good forecasters. Philip Tetlock's long-term study of political science specialists has shown that specialists are not significantly better than non-specialists at predicting the future. Indeed, the bigger the name the worse the forecasts. "Experts in demand," Tetlock says, "were more overconfident than their colleagues who eked out existences far from the limelight."¹⁵

International Relations, then, is not given to futurology. Here is a discipline that achieved prominence in the rationale of the Cold War, failed to anticipate its end, and has been struggling to adjust ever since, with significant consequences for its viability as a distinct academic discipline.

All this has happened in parallel with a fundamental transformation in our ability to create and share knowledge. What we are now witnessing is the latest phase of a six hundred year process which, starting with the Renaissance and moving on to the Reformation and the Enlightenment, has sought to break the monopoly of knowledge

¹³ Ibid p.73

¹⁴ UC Berkeley economist and Google consultant Hal Varian estimates that information is growing 10 times faster than any other product on the planet. "Why do we still have big questions?", Kevin Kelly, *Wired*, 1 February 2007.

¹⁵ "Everybody's an Expert: Putting Predictions to the Test", Louis Menand, *The New Yorker*, 5 December 2005, http://www.newyorker.com/critics/books/articles/051205crbo_books1.

held first by the Catholic Church and then assumed, presumptively, by the institutions of government and academia.

Thanks to the Internet, knowledge of international affairs – indeed of any discipline – is the common inheritance of every human being (assuming they have the means to access this). The democratization of knowledge, like the democratization of politics, renders unto the individual both heightened responsibility and the opportunity to exercise greater influence in the conduct of his – or other – governments.

Moreover, it has blunted the technological edge enjoyed by the West. For the cost of a PC and an Internet connection, and with sufficient training in how to use both, it is possible to acquire a high level of knowledge and expertise on any subject. The Internet recognizes no elites, nor is it concerned with one's previous academic qualifications. Users who find something above their level of comprehension will migrate to something simpler, and vice versa. In the end, all that matters is whether the information can furnish learning and action.

The Terrorist Group as Learning Organization

This new paradigm can best be seen in the manner in which it has been embraced by terrorist organizations around the globe. Al-Qaida, Hamas and others are now seen to embody the best practices of the learning organization.¹⁶ Their ability to create and transfer knowledge across territorial, linguistic, and even ideological boundaries has made them a difficult adversary to confront.

Indeed, for many terrorist organizations, the Internet is a means to an end. Given the amount of publicly available information, investing time in online research – identifying targets, communicating with sponsors, developing explosives using Internet blueprints – is likely to prove more valuable than developing a sophisticated cyber-attack portfolio.

After seized computers in Afghanistan revealed that terrorists had been using the Web for research and planning, former US Secretary of Defense Donald Rumsfeld issued a memo to the US Department of Defense ordering changes in cyber security in which he quoted from the so-called Manchester Manual (an al-Qaida training primer), that “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy.”¹⁷ In addition, captured equipment and literature has revealed that al-Qaida operatives are well versed in technology and engineering.¹⁸ Support cells have sprung up across the Web, and sites and chat rooms

¹⁶ An excellent definition of organizational learning as related to terrorism reads as follows: “The process through which members of a group acquire new knowledge that can be applied in strategic decision-making, tactical planning or design, and operational activities.” Brian A. Jackson, *Organizational Learning and Terrorist Groups*, RAND Working Paper WR-133-NIJ, February 2004. See also, Brian A. Jackson et al, *Aptitude for Destruction Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, RAND Corporation, 2005.

¹⁷ “Citing Al Qaeda Manual, Rumsfeld Re-Emphasizes Web Security,” *InsideDefense.com* (15 January 2003); <<http://www.insidedefense.com/>>.

¹⁸ Clay Wilson “Terrorist Capabilities for Cyber-attack,” in *International CIIP Handbook 2006*, Vol. 2,

have been used to acquire knowledge on targets, American interests, and training.¹⁹

Law enforcement and intelligence agencies assert that a number of cases have been uncovered in which jihadist cells appear to have formed among like-minded strangers who met online, and there appear to be many other cases in which relationships built in the real world have been sustained and nurtured by the Internet.²⁰ Additionally, the Web has served as a virtual replacement for physical training camps and as a repository of jihadist thinking.^{21 22} The Web has helped al-Qaida grow both its network and its finances. According to Rita Katz of the SITE Institute, which monitors jihadist Web sites, “If you want to conduct an attack, you will find what you need on the Internet” (quoted in Coll and Glasser, 2005). Additionally, there is clear evidence that al-Qaida and its offshoots are using the Internet for tactical and intelligence purposes. According to recent reports from the Critical Infrastructure Protection Board (CIPB), which operates under the Department of Homeland Security, computers “from the Mideast are probing American electric, water, and energy systems, and seem especially interested in gaining access to nuclear-power plants.”²³ Such reports mesh with earlier concerns uncovered by law enforcement agencies in California of probes against Silicon Valley companies and Bay Area infrastructures, also originating from computers in the Middle East and South Asia.²⁴ In terms of knowledge sharing, there is ample evidence that terrorists are also using the Web to increase their collective ability to promote their agenda and to do greater harm.

Clearly, the West’s information edge has not deterred its adversaries from using the same tools to improve their operational and tactical knowledge. Nor has it prevented them from acquiring new knowledge, sharing it with likeminded individuals, and applying it to a desired end. Indeed, recent research argues that international terrorist groups have created a global knowledge network through which tactics and strategies are increasingly shared.²⁵ The increased lethality of improvised explosive devices, for example, can be attributed, in part, to the willingness and ability of terrorist and insurgent groups to share knowledge via the Internet.²⁶ The Internet has become a primary learning, training and collaboration resource for terrorist groups around the world: log on, tune in, blow up.

eds. Myriam Dunn and Victor Mauer (Zurich: Center for Security Studies), 2006.

¹⁹ Rohan Gunaratna “Responding to the Post 9/11 Structural and Operational Challenges of Global Jihad,” *Connections* (Spring), 2005.

²⁰ Steve Coll, Susan Glasser “Terrorists Turn to the Web as Base of Operations,” *The Washington Post* (7 August 2005).

²¹ “Al-Qaeda Online: Understanding Jihadist Internet Infrastructure,” *Jane’s Intelligence Review*, 1 January 2006, <http://www.nupi.no/IPS/filestore/Lia2005Al-Qaeda_online_und_75416a.pdf>.

²² NewsHour with Jim Lehrer (2005), “Online Terrorism,” discussion with Neil Doyle and Paul Davies, 2 August 2005; <http://www.pbs.org/newshour/bb/terrorism/july-dec05/online_8-02.html>.

²³ James Robbins “The Jihad Online: Mouse Clicking Your Way to Martyrdom,” *National Review Online*, 30 June 2002, <<http://www.nationalreview.com/robbins/robbins073002.asp>>.

²⁴ Barton Gellman “Cyber-Attacks by Al Qaeda Feared,” *The Washington Post* (27 June 2002).

²⁵ James Forest ed. *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*, Rowman and Littlefield, May 2005, Preface p.xi.

²⁶ The IED Marketplace in Iraq, John Robb, *Global Guerrillas Blog*, 3 August 2005, <http://globalguerrillas.typepad.com/globalguerrillas/2005/08/the_ied_marketp.html>.

Harnessing the Knowledge Revolution

So how should the discipline respond to the new knowledge paradigm? One would assume that given its interdisciplinary and heterogeneous nature, no subject would be better suited to helping us understand the forces shaping our planet. And yet, to the outside observer, it appears worryingly inadequate to the task and dangerously behind the times in the fields of knowledge sharing and collaborative learning.

We contend that what's needed is an altogether different approach in the teaching and conduct of IR as an academic discipline, one that's more accommodating of open source learning and publishing methodologies. Such an approach should enable improved understanding of the many complex, interrelated challenges we face. It should also furnish the next generation of IR and security policy graduates with the practical and cognitive skills that will enable them to perform more effectively in the international marketplace.

Of course, it is tempting to throw one's hands up in despair at the challenges currently faced by the IR scholar without having to add anything more to their plate. But none of these challenges are new. Writing in 1949, one scholar described IR as a "vast, sprawling field... the subject of endless writing and comment".²⁷ The author laments the endless stream of books, memoirs, documents, newspapers, and government reports that one must read to master the discipline. Worse, if the student limits his interests and investigations to certain geographic areas, he is acutely conscious of the inter-relationship between what happens in his chosen field and developments outside in the terra incognita.²⁸ The IR scholar, he concluded, cannot master the entire field and cannot safely limit himself to narrow specialization.²⁹ More than half a century on, little seems to have changed. But the challenge of understanding the world and the dangers inherent in failing to do so – particularly in the nuclear age – are much greater than at any time before.

Open Source Knowledge, Open Source Learning

A first step in this direction would be to harness the benefits offered by open source learning environments. The last decade has seen the evolution of the Internet from an information-based publishing platform to a knowledge-based learning platform. It is now possible for any individual to go online and contribute what they know to a common pool of knowledge. This knowledge can be reviewed, revised, repackaged and redistributed in any number of forms – a news article, a research paper, a learning module or an anecdote. Almost simultaneously, we have witnessed the emergence of a global learningscape –

²⁷ Grayson Kirk, Materials for the Study of International Relations, *World Politics*, Vol. 1, No. 3 (April 1949) p.436.

²⁸ Ibid.

²⁹ Ibid.

one that's daily enriched by interplay between the cognitive and social bases of learning.³⁰

This learningscape – currently best exemplified by the *Wikipedia* project - is a flexible and extensible learner-centric environment that provides tools, resources and community support around one or more subjects.³¹ The success of *Wikipedia* and its philosophy hasn't been lost on the US intelligence community; in October 2006 it announced the launch of *Intellipedia*³², a wiki-based platform for greater knowledge sharing, data synthesis and collaborative exchange. By using wiki technology, the US intelligence community is hoping to leverage its intellectual assets in a collaborative way for the production of national intelligence estimates and other key reports. While this is a positive step, much remains to be done and academia is central to improving efforts in this domain.

Open learning environments such as these are proving a rich resource for both amateurs and professionals looking to connect with and learn from one another. Moreover, they offer a form of “cognitive apprenticeship” where one's ideas are tested and refined in an ongoing dialog with one's peers.³³ Participants who engage in such environments are acquiring skills that will enable them to prosper in an information rich environment, to connect different strands of learning and thought and, most importantly, to deliver a product that is of practical value to the end user. Although we might not want to admit it, the cognitive challenge of participating in an online learningscape is quite unlike anything offered by the traditional academy.

By contrast most graduate research in IR and the humanities tends to be solitary in nature. With the exception of an occasional research symposium or conference presentation, interaction with one's peers is typically kept to a minimum. Few of these ideas ever enter the public domain or are subject to public scrutiny. Unfortunately, 15 minute poster board presentations are as public as most graduate research proposals get.

In the end, the validity of a graduate research program is only properly assessed by the professor charged with supervising it. A small number of (heavily edited) theses are accepted for publication in scholarly journals. Fewer still go on to be published in their entirety with a print run in the low hundreds. And the odd exception goes on to become the basis for “popular” literature. The majority, however, no matter how original, penetrating or incisive, disappear into university annexes.

³⁰ John Seely Brown, *New Learning Environments in the 21st Century: Exploring the Edge* (2005), accessed at <<http://www.educause.edu/ir/library/pdf/ff0604S.pdf>>.

³¹ Definition adapted from the Learningscapes Wiki, University of Winnipeg <<http://wiki.uwinnipeg.ca/index.php/LearningScapes>>.

³² See, Clive Thompson, *Open Source Spying*, New York Times, 3 December 2006; also, *Government Unveils Wikipedia for Spies*, Reuters, 31 October 2006, accessed at <<http://www.msnbc.msn.com/id/15503834/>>.

³³ John Seely Brown, “The Social Life of Learning: How can Continuing Education be Reconfigured in the Future?” in *Continuing Higher Education Review*, Vol. 66 (2002) p. 59.

Elsewhere, the idea of collaborative learning and knowledge sharing is met with alarm. Why would anyone publish their research proposal or interim findings if there was a risk of this being stolen? Invariably, the emphasis is on what one stands to lose rather than what one hopes to gain. This is to miss the point entirely. Intellectual enquiry has always been a matter of public exchange and has always prospered as a result of it. Indeed, the public exchange of knowledge was historically seen as a primary duty of the learned elites.

There is sufficient historical precedent here. The printing presses of early modern Europe served as a meeting place for scholars, academics, writers and others to meet and discuss the issues of the day. These establishments facilitated intellectual enquiry and social networking, which in turn hastened the development of new ideas, new paths of enquiry, and the rapid creation, acquisition and distribution of knowledge.³⁴

In line with this thinking, there needs to be a profound change of attitudes towards the merit of online and open access research and publishing. At present, the IR community tends to regard digital publications – regardless of their quality or whether they have been peer reviewed or not – as inferior to print based journals. Similarly, they do not factor as highly as print based publications when it comes to securing tenure or promotion. Professional recognition of open source publishing and the value of contributing to open learning environments and other knowledge sharing networks would be an important step towards leveraging the power of the Internet to maximize the reach of IR scholarship. Naturally, for online journals there would need to be clear guidelines with regard to online peer review. But the author should also be given the choice of submitting his work to broader public scrutiny too, if only as a means of furthering public knowledge. This is not to argue against traditional publishing modules. Quite the contrary; but there should be greater acceptance of digital publishing models and their potential reach.

Furthermore, encouraging the use of blogs, wikis and other collaborative tools should be a matter of course in academia. These are the modern equivalents of the 15th century printing presses and the coffee houses of pre-revolutionary Europe. Students could be tasked with providing status reports on their research activities using public blogs that could also serve to invite input from others.

Academia should also encourage the creation and growth of online communities that are dedicated to specific topics or issues. These communities could serve as information filters, knowledge sharing platforms, and online classrooms for researchers, policy analysts, students and others. Ideally, these communities should be networked to allow for interdisciplinary collaboration and exchange, and would also be open to the general public so that they too could advance their knowledge.

Love it or hate it, the success of *Wikipedia* has demonstrated the value of collaborative communities and their ability to make waves. In 2005, when science entries in *Encyclopedia Britannica* were compared – rather unfavorably for them – against

³⁴ Michael Hauben, *The Expanding Commonwealth of Learning: Printing and the Net*, <<http://www.columbia.edu/~rh120/ch106.x16>>.

Wikipedia the furor from the professional publishing world was palpable. *Nature*, the journal that conducted the review, found that on average a *Wikipedia* science entry averaged four inaccuracies while *Encyclopedia Britannica* averaged around three.³⁵ The *Nature* survey demonstrated that while *Wikipedia* was not immune to errors, neither were the experts.

With regard to terrorism, it has often been said that it takes a network to defeat a network. But while there are thousands of excellent websites on everything from arms control to transport security, precious few are connected, and fewer still allow for any form of public participation, knowledge generation, or social networking. Efforts to synthesize this vast catalogue of information resources, to open its riches to public scrutiny and distributed peer review, and to enable further collaboration and knowledge creation are sorely needed.

The International Relations Knowledge Worker

The growing complexity of our world also requires a new set of skills for people working in international relations, security policy and intelligence. Many of these fall under the banner of information or IT literacy and, we contend, should be part of a student's formal education at university.

At present, many of us are trying to manage 21st century information flows with 19th century intellectual skills.³⁶ As a matter of necessity, people working in international relations should be given the skills needed to thrive in knowledge rich environments. Training in how to locate, organize, analyze, synthesize and present knowledge from print, electronic and other resources is essential to working in an increasingly knowledge driven workplace. Moreover, they should be able to work with large volumes of data and identify patterns and connections among seemingly unrelated information.³⁷

Similarly, knowledge of the latest IT tools and technologies is an essential prerequisite to generating knowledge and sharing this in open learning environments. The ability to create simple web pages, audio files and other educational materials is key to ensuring the spread of knowledge beyond one's own circle of acquaintances.

These skills should be part of every academic or professional training program for people studying or working in the IR and security policy community. Graduate students, for example, should be encouraged to use the Internet to promote both their research and themselves. Doing so would allow them to engage in an ongoing process of learning, dialog and collaboration. It would also encourage interdisciplinary exchange, social networking and the discovery of new research paths.

³⁵ For more on the study, read: <<http://www.nature.com/nature/journal/v438/n7070/full/438900a.html>> and for the official objection and responses to it, see: <<http://www.nature.com/nature/britannica/index.html>>.

³⁶ Paul Saffo, Information Surfing, *Personal Computing*, July 1989, accessed at <<http://www.saffo.com/essays/infosurfing.php>>.

³⁷ Ibid.

Indeed, what is needed is a new kind of international relations knowledge worker. This is an extension of the term coined by the late management guru Peter Drucker. For Drucker, knowledge workers are people who use what they know to produce new information, ideas and concepts.³⁸ Taking it a step further, we would call this person the IR synthesist.

The IR synthesist would be someone who works in the IR or the security policy domain, and is paid to leverage their intellectual assets for the good of their project, organization or other goal. In addition, these individuals would be exceptionally well read and informed; they would have excellent source awareness and information/knowledge management skills; they would be capable of synthesizing vast amounts of information into knowledge that can be accessed and used by others; they would have high language proficiency and cultural sensitivity; they would have excellent networking skills, know who the experts are and where they stand on the major IR and security issues; and they would be given a range of cognitive skills that allow for flexible and original thinking.

Cultivating such individuals may sound like a tall order, but in fact, these are the skills employers everywhere are asking for. Expanding the IR curriculum to allow for greater emphasis on practical skills such as IT and information literacy and, most importantly, languages, would be a positive step and one that would yield an enormous return over time. Moreover, it would give future IR professionals the ability to move from an information to a knowledge-based world.

To Conclude

This paper has laid out some tentative arguments with respect to the conduct and study of international relations in a knowledge driven age. Our thesis contends that information has been supplanted by knowledge as a key determinant of one's ability to project power or affect traditional power structures. This is evident in terrorists' use of the Internet to sharpen their learning and share what they know.

In response to these developments, the IR and security policy community must recognize the importance of knowledge over mere information and must galvanize itself to take full advantage of today's open source learning environments, namely: networked collaboration; distributed, independent and rapid peer review; social networking; the ability to leverage the collective intelligence of a broad range of actors; community building; and heightened learning. Such environments should be cultivated as a means of improving dialog and knowledge exchange in the IR and security domains. Failure to do so is likely to limit our ability to cultivate innovative solutions to 21st century security threats.

Finally, we have argued for a reappraisal of the skills needed by international relations graduates and others working in the field. Given the importance of lifelong learning, sharing and collaboration – and of countering the challenges we face at the turn of the century – it is essential that these skills become part of the standard IR curriculum and other professional training programs.

³⁸ Peter Drucker, "Focus on Competition" *The Essential Drucker*, Collins Business Press 2001, p.212.