A Compilation of Richard U. Wheeler's Writings 2007 to 2011

The Truman National Security Project

National Security is a Litmus Test for Leadership
Understanding national security is a litmus test for leadership. The Truman National Security Project is a national security leadership institute, the nation's only organization that recruits, trains, and positions a new generation of progressives across America to lead on national security.

Our mission is to provide the skills, knowledge, and network to create an influential force of leaders across the country who advance strong progressive national security policy through advocacy initiatives, media appearances, and public service in elected and appointed office.

Today you will find leaders we have trained running for office across the country, advising presidential and Congressional campaigns, drafting legislation in the halls of Congress, appearing on national television and radio, and advocating for smart policies in your state legislature.

Richard U. Wheeler is a Truman National Security Fellow

WIRED's Danger Room

WIRED is the first word on how ideas and innovation are changing the world. Each month in the magazine and every day online, our editors deliver a glimpse into the future of business, culture, innovation, and science. AdWeek named WIRED to its 2011 Hot List and made WIRED its first-ever "Magazine of the Decade" in 2010. It was named to Advertising Age's A-List in 2010, received three National Magazine Awards for general excellence in 2005, 2007, and 2009, and was nominated for a National Magazine Award for Magazine of the Year in 2011. Wired.com was named 2009's Best Magazine Website by AdWeek, Best News, Business & Finance Website in 2009 by MPA Digital, and was a 2011 National Magazine Award for Digital Media "General Excellence" finalist. WIRED and Wired.com reach more than 14 million readers each month.

The Danger Room is a sub-category of SECURITY on the WIRED web site.

Richard U. Wheeler is a contributor to WIRED's Danger Room.

Here's What Bond's First Flick Got Right About Spycraft, 50 Years Later

In WIRED's Danger Room
By Richard Wheeler
October 12, 2012 10:00 AM

The original movie poster for "Dr. No." Courtesy: United Artists

50 years ago today was the cinematic birth of the man who everyone thinks of when they think about spies: James Bond. Dr. No was released Oct. 5, 1962, and ever since James Bond has been synonymous with espionage — much to the chagrin of actual spooks, who have to work in tedious State Department cover jobs processing visa applications and recruit low-level stooges more than they get to ride around in posh cars and bed amorous, well, Bond girls. And it doesn't matter which government you work for: You're going to be staying in a Marriott and the per diem on travel is not going to cover those bottles of Dom Pérignon.

The early Bond films can also seem quaint to audiences today, especially when compared to the muscular antics of Daniel Craig crashing through a wall in Casino Royale or the endless Inosanto Lacoste-inspired fight scenes from the Bourne movies. Let's face it: The old Bond would get his ass handed to him by today's Bond, and in a world where everyone is more crazy

about SEAL Team 6 and robots than they are about old-fashioned spies, it's not even clear that people care too much about today's Bond.

But a close reading of Dr. No reveals that Ian Fleming's insights into the real nature of intelligence work remain valid even today. When you strip away the gadgets, and the glamour, and the sex, what remains are some surprisingly real observations about the real secret world of intelligence.

Let's take a look at one scene from the beginning of the movie as an example:

INTERIOR, MI6 HEADQUARTERS, M'S OFFICE, NIGHT
M and JAMES BOND are meeting, and M has called in MAJ BOOTHROYD, an armourer. BOND has just come from a London casino and is wearing a tuxedo.

M
[to JAMES BOND]
Take off your jacket.

[BOND removes his dinner jacket to reveal a shoulder holster]
Give me your gun.

[BOND hands M his pistol]
Yes, I thought so. This damn Beretta again. I've told you about this before.

[to MAJ BOOTHROYD]
You tell him … for the last time.

MAJ BOOTHROYD
[Examining BOND's pistol]
Nice and light … in a lady's handbag. No stopping power.

M
Any comments, 007?

JAMES BOND
I disagree, sir. I've used a Beretta for ten years. I've never missed with it yet.

M
Maybe not, but it jammed on your last job and you spent six months in hospital. A double-0 number means you're licensed to kill, not get killed. And another thing. Since I've been head of MI6, there's been a 40% drop in double-0 casualties. I want it to stay that way. You'll carry the Walther… Unless you'd prefer to go back to standard intelligence duties?

JAMES BOND
[with emphasis]

No, sir. I would not.

M
Then from now on you carry a different gun. Show him, armourer.

MAJ BOOTHROYD
Walther PPK. 7.65mm with a delivery like a brick through a plate-glass window. Takes a Brausch silencer, with little reduction in muzzle velocity. The American CIA swear by them.

A scene from the latest James Bond movie, "Skyfall." Courtesy: MGM

Here are just a few of the things that you can learn from this tiny bit of film:

1) Intelligence officers try too hard to be cool. (Bond was just out at a London casino playing baccarat with a pistol in shoulder holster…. Really?)

2) Intelligence officers habitually fail to follow orders. ("Yes, I thought so. This damn Beretta again. I've told you about this before….")

3) High-level management micromanages. (Same quote: Why is the head of MI6 giving direct orders to a field officer about what weapon to carry? That's like the director of CIA giving a 28-year-old case officer an order about what weapon to carry in Afghanistan … and this is sometimes pretty close to what really happens.)

4) Even when they micromanage, managers use intermediaries to insulate themselves from blame. ("You tell him … for the last time….")

5) Subtlety is effeminate, and this is a man's game. ("Nice and light … in a lady's handbag. No stopping power…." Intelligence can roughly be split into two large camps: supernerds who like to figure things out, and superjocks who like to kick ass. But everybody is pretty clear that the superjocks are the coolest, and if one has any sense at all one tries to jump ship to that team at the earliest opportunity.)

6) Job titles and job descriptions are important: You are allowed to do what is in your job description but not allowed to stray outside of it. ("A double-0 number means you're licensed to kill, not get killed….")

7) Metrics matter! ("Since I've been head of M6, there's been a 40% drop in double-0 casualties. I want it to stay that way." I mean you don't just get a knighthood for nothing….)

8) "Standard intelligence duties" are boring: Why else would a return to doing them be a sufficient threat to secure cooperation?

9) Brute power ("…a delivery like a brick through a plate-glass window…") is more important than accuracy or experience ("I've used a Beretta for ten years. I've never missed with it yet…").

10) Everyone is obsessed with what the CIA is doing and is convinced that they are right.

Of course after Dr. No the realism in the Bond films steadily decreased, as audiences became captivated with all the glitz and glamour that we've come to associate with the Bond franchise. Perhaps the newest Bond, Skyfall, which is set for release later this month, manages to capture some of the old Fleming flair for the real—but I doubt it.

How to Talk Like a Pirate … in His Native Javanese

In WIRED's Danger Room
By Richard Wheeler
September 19, 2012 10:59 AM

Indonesian Navy commandos detain mock pirates during a 2001 exercise in the Malacca Straits. Photo: AP/Ed Wray

International Talk Like a Pirate Day is here again for its 10th anniversary. Which means the old gags — shivering your timbers, calling out to your maties, mispronouncing "Sarsgaard" — are getting kind of stale, especially when there are real-life pirates roaming the high seas. If you really want to rap like a modern-day Captain Jack, it means learning a few choices phrases in a new language – one spoken by the gents hijacking ships right now.

Last year Danger Room's hard-hitting ITLAPD coverage brought you linguistic quick guides to Somali and Yemeni Arabic. But since then pirate attacks off the Horn of Africa have dropped significantly, especially over this past summer. Some credit may be to the weather, since it turns out that rough seas during monsoon season restrict the ability of Somali pirates to operate. Some credit may also be to the combined efforts of various anti-piracy forces, including those of the United States and the EU, which have stepped up attacks against pirates in the past year. And some credit may be to increased security measures on ships that are passing through the Gulf of

Aden and around the Horn of Africa — a trend which continues results reported in 2011. But whatever the reasons, the facts are that attacks are down, and so you may be starting to wonder if all the that time you've spent in the last year learning pirate phrases in Somali was worth it. You may even be wondering if it's worth it to talk like a pirate at all.

Well matorka demee, sailor! Just because piracy is down around Somalia doesn't mean the high seas are safe for mariners the world over. While the drop in Somali piracy has reduced the rate of piracy globally, piracy remains high in the number-two region for pirate activity in the world: Southeast Asia and the Indian sub-continent. And the number-one area for pirate activity in the region remains Indonesia. In the first half of 2012 there were 32 attacks in Indonesia, one in the Malacca Straits, and four in Malaysia — compared to 21, zero and 11 for all of 2011. If piracy continues at the same rate for the rest of 2012 we can expect a record year for piracy in the region, continuing a trend that started at an all time low mark for piracy in the region in 2009.

So it's time to learn a little pirate Indonesian, me hearties.

	Guide	Section	English	Bahasa Translite ration	Bahasa	Malay Translite ration	Malay	Javanese Translite ration	Javanese
1	Navy	Bridge Commands	Where is the control room?	dee mana kamar pengawas ?	Di mana kamar pengawas ?	dee maanaa beeleyk kaawaalaa n?	Di mana bilik kawalan?	Roowaan g kontRolee poon wonten poondee?	Ruang kontrolipu n wonten pundi?
2	Navy	Bridge Commands	Stop the engines!	maateeka n mesinyaa!	Matikan mesinnya!	henteekaa n enjeen!	Hentikan enjin!	masin eepoon deepoon pajaahee!	Mesinipu n dipunpeja hi!
3	Navy	Bridge Commands	Where is the captain?	dee mana paa kaapten?	Di mana pak Kapten?	dee maanaa kepten aandaa?	Di mana kapten anda?	kaapten eepoon wonten poondee?	Kaptenipu n wonten pundi?
4	Navy	Prisoner Questions	Who is the captain?	seeyahpah kaptenyaa ?	Siapa Kaptenny a?	siyaapaa keptenyaa ?	Siapa kaptennya ?	kaapten eepoon seenten?	Kaptenipu n sinten?
5	Navy	Bridge Commands	How many men are on this ship?	berapa orang ana boo-ah kapaal kapaal inee?	Berapa orang (anak buah kapal) kapal ini?	buraapaa raamaay aanaak kaapaal daalaam kaapaal inee?	Berapa ramai anak kapal dalam kapal ini?	teeyaang peentin wonten kaapaal pooneeko ?	Tiyang pinten wonten kapal punika?
6	Navy	Questions and Needs	Do you have weapons?	ahpahkah andah poonya senjaataa?	Apakah anda punya senjata?	aandaa aadaa senjaataa?	Anda ada senjata?	poonopo paanjenen gaan kaagoong aan senjaataa?	Punapa panjeneng an kagungan senjata?
7	Navy	Bridge Commands	Where are the weapons?	dee mana senjataa senjataan yaa?	Di mana senjatasen jatanya?	dee maanaa senjaataa-senjaataa eetoo?	Di mana senjata-senjata itu?	senjaataan eepoon wonten poondee?	Senjatanip un wonten pundi?
8	Navy	Critical Commands	Do not resist!	jangan malaawan !	Jangan melawan!	jangaan melaawaa n!	Jangan melawan!	aampoon nglaawaa n!	Ampun nglawan!
9	Navy	Critical Commands	Don't move!	jangan bergeraa!	Jangan bergerak!	jaangaan burguraak !	Jangan bergerak!	aampoon obah!	Ampun obah!
10	Navy	Critical Commands	Come here!	kemahree !	Kemari!	daataang sinee!	Datang sini!	mReekee!	Mriki!

11	Navy	Critical Commands	Hands up!	aangkat tangan!	Angkat tangan!	aang-kaat taangaan!	Angkat tangan!	aang kaat taangaan!	Angkat tangan!
12	Navy	Critical Commands	Don't look at me!	jangan leehaat sahyah!	Jangan lihat saya!	jaangaan paandaang saayaa!	Jangan pandang saya!	aampoon namaatken koolo!	Ampun namatken kula!
13	Navy	Critical Commands	Look forward!	leehat looroos ke depan!	Lihat lurus ke depan!	leehaat ke haadaapaan!	Lihat ke hadapan!	neengaale e ngaaching!	Ningali ngajeng!
14	Navy	Critical Commands	Close your eyes!	choba tootoop mataanya!	Coba tutup matanya!	tootoop maataa aandaa!	Tutup mata anda!	mReepaat eepoon deepoon tootoop!	Mripatipun dipuntutup!
15	Navy	Critical Commands	Kneel!	choba berlootut!	Coba berlutut!	melootoot!	Melutut!	jong ko!	Jongkok!
16	Navy	Critical Commands	Hands behind your head!	tarooh tangan andah dee belakang kepaala!	Taruh tangan anda di belakang kepala!	taangaan dee belaakaang kepaalaa!	Tangan di belakang kepala!	taangaan neng mbooRee seeRah!	Tangan neng mburi sirah!
17	Aircrew	Emergency Transmissions	We have a problem.	ahdah maasalaa	Ada masalah	aadaa maasaalaah	Ada masalah.	wonten maasaalah	Wonten masalah
18	Basic	Commands, Warnings and Instructions	Stop!	burhentee!	Berhenti!	burhentee!	Berhenti!	maandek!	mandhek!
19	Basic	Commands, Warnings and Instructions	Stop or I will shoot.	burhentee naantee sahya tembaak	Berhenti nanti saya tembak.	burhentee aataaw saaya aakaan teymbaak!	Berhenti atau saya akan tembak!	maandek yen oRa maandek, taa tembaa	mandhek yen ora mandhek, tak tembak
20	Basic	Commands, Warnings and Instructions	Surrender	menyerah laa	Menyerah lah	suraah deeree	Serah diri.	nyeRah	nyerah

But Indonesia has over 700 languages, so where should you start? Well the United States Department of Defense's Defense Language Institute focuses on three: Bahasa Indonesian, Javanese, and Malay. Bahasa Indonesian, a language similar to Malay, is the official language of Indonesia, spoken by nearly 50 percent of the population, and the primary language of a little more than 10 percent of the population. Javanese the second most widely used language, is spoken by approximately 40 percent of the population. Finally, Malay, which has at least 14 dialects and nearly 40 million speakers throughout the region, is the official language of Malaysia and is also widely spoken in Sumatra, the largest of Indonesia's northern islands which lies across the pirate prone Straits of Malacca.

But enough of the ethnography lessons: Let's start talking like an Indonesian pirate! Berhenti atau saya akan tembak!

Report from Tehachapi: Why Wind Power Means Jobs, Security

in The Truman National Security Project
By Richard Wheeler August 16, 2012

The Official Opening of Scout Moor Wind Farm

Last week I accompanied a group of veterans who are part of Operation Free on a trip to Tehachapi, CA, located just on the edge of the Mojave Desert in southern California, to learn about wind. There's a lot of it in Tehachapi — a name that many believe comes from the Kawaiisu word tihachipia, which means "hard climb" — a rugged and mountainous country that was the site of some of the first large scale commercial wind production development nearly 30 years ago, and is the site of continued innovation in developing America's clean and secure energy future. A future that is threatened unless Congress moves to allow industry to continue to develop and grow this proven, dependable, and clean energy technology by renewing the wind Production Tax Credit (PTC)

We were in Tehachapi to visit Airstreams Renewables, a company founded by wind industry veterans to train wind turbine technicians. The Airstreams course puts trainees through an intensive 25-day, 200-hour program that qualifies them for technician jobs in the wind industry. These jobs can pay anywhere from $50,000 for technicians who work locally to over $100,000 for those who travel. And thanks to Airstreams' work with city and county veterans support groups and the United States Department of Veterans Affairs, military veterans can use their GI Bill benefits to pay for the entire course. It's welcome news for veterans in Kern County, where Tehachapi is located, which is running unemployment rates of more than 20%, as well as for those around the country who live in growing footprint of the wind industry.

I talked to Dave Schulgen, Chairman and CEO of Airstreams and a Marine Corps veteran, about future growth at Airstreams and in the wind industry as a whole. “We’re on track to train 500 technicians a year,” Shulgen told me, “and the industry still needs more.” Shulgen estimated that the current demand is for nearly 2,000 new technicians a year. That’s part of the estimated 100,000 jobs that wind production is estimated to produce in the next four years. Jobs that include not just the technician jobs that Airstreams graduates fill but also highly skilled manufacturing jobs. 60% of the components of wind turbines used in the United States are made here, and wind energy component production has already completely revitalized entire towns that were threatened with losing their manufacturing job base.

Part of the reason for this growth is the Production Tax Credit (PTC). The PTC gives wind producers a 2.2 cent tax credit for every kilowatt hour of energy that they produce. It isn’t a subsidy or a hand-out as producers are credited only for energy produced. The PTC merely reduces their tax burden slightly as a way to spur innovation, growth, and ultimately jobs — like the technician jobs that Airstreams’ graduates are working in right now. The PTC has broad bipartisan support, with backing from Republicans like Ron Paul and Newt Gingrich and form Democrats including President Obama. In a December 2011 event in Iowa, Gingrich advocated for a ten-year-time horizon on the PTC, saying in part, “One of the major problems we have with renewable policies is that the time horizon on the tax credits is too short, and the degree to which they caught up in congressional politics leads to a sort of an up-and-down effect so you can’t get capital investment over time.”

The long-term effects of PTC are already starting to pay off for Airstreams, where a few weeks ago an early graduate from when the program started three years ago started working as an instructor. The ability to build and grow upon knowledge is essential in any industry, and the PTC has helped the wind industry use it’s experience to lower the cost of wind production by nearly 90% in the past decade. Today wind powers nearly 12.8 million American homes, and does so while creating American jobs and reducing America’s dependance on foreign energy sources. The PTC is also helping America create a wind industry that is competitive with foreign efforts. Wind technology is a major area of investment in China and throughout Europe, where government support far outstrips that of the United States. The relatively small bit of tax relief provided by the PTC helps American business compete in this worldwide arena.

Renewing the PTC can protect these gains and create more for the future. At a time when American communities are looking for new jobs and the American wind industry is looking to make them, it would be a shame to lose this opportunity.

Richard Wheeler is a Truman Security Fellow.

Turn Left Here? Why Problems with GPS Show our Cyber Weaknesses

in The Truman National Security Project
By Richard Wheeler August 1, 2012

image from Flowizm

It turns out that the problems with GPS are bigger than any of us knew about — and that has serious implications about not just GPS, but about the larger cybersecurity debate that is playing out in the Senate this week with the final debate over the revised Cybersecurity Act of 2012.

Last month news broke that a team of researchers from the University of Texas had hijacked a drone by spoofing the GPS used in it's navigation system. "Spoofing" is a hacking technique that involves fooling a computer into believing that the hacker's computer is a trusted computer. In this case, the U of T team fooled the drone by sending a signal that pretended to be from satellites in the GPS constellation but contained inaccurate location information — information that would have caused the drone to crash if not for pilot intervention.

Which should worry you not just because GPS helps fly drones but also because none of us know how to get anywhere without it any more.

Earlier last month the GPS industry successfully fought off the perceived threat that part of the electromagnetic spectrum used by GPS might be taken by other services. But this threat pales in comparison to the threat of GPS spoofing. GPS is both a critical military technology — as evidenced by the Department of Defense's strategic budget priorities and the continued

restrictions imposed by the Department of Defense and the Department of State on the export of military grade GPS receivers and associated technology.

Despite this, there doesn't seem to be a consensus which part of the federal government should take the lead on address the issue. Even though Congress recently passed a new bill instructing the Federal Aviation Administration to increase the use of GPS in aerial navigation and open United States airspace to privately owned drones, the FAA has no authority to secure the GPS signal. Similarly, although the Department of Homeland Security has been assigned the lead role in domestic cybersecurity, DHS was absent at a recent House of Representatives hearing on domestic drone security that specifically addressed the GPS vulnerability. All this despite the fact that this is the second (known) time that drones have been hacked.

All this goes to show that the United States still has a long way to go in figuring out how to secure itself and its critical infrastructure from cyber attack. And the revised Cyber Security Act of 2012 is least that we can do to get that process moving faster. The current version removed language that some business leaders felt would create burdensome regulation, and now requires additional regulation only of some already heavily regulated critical infrastructure industries like nuclear power — in short, industries where we can all agree that there cannot be too much safety and security since the cost of failure is higher than we want to bear (think Fukushima or New Orleans and you'll see what I mean). Both House and Senate leaders on both sides of the aisle — including the House Republican Task Force on Cybersecurity — and President Obama, all agree that the current bill is good enough to start the ball rolling on making positive changes.

And since I don't think I'm going to give up my GPS — no matter how much that may be a good idea — we can't get started soon enough.

Richard Wheeler is a Truman Security Fellow.

The Senate Cybersecurity Bill: A Start, But Not an Answer

in The Truman National Security Project
By Richard Wheeler July 17, 2012

It has become a depressing but now familiar pattern: in the space of a week, reports surfaced both that LinkedIn's mobile app scraped information from users' mobile devices and stored it on LinkedIn's servers—without informing it's users of the practice—and that LinkedIn user passwords had been broken and stolen by hackers since LinkedIn had only lightly encrypted and poorly defended the data. To make matters worse, like many of the similar breaches of recent years, these weren't discovered or disclosed by LInkedIn but by private security researchers.

There are a number of concerns here, but one of the biggest is that for many workers today LinkedIn has become part of their "critical infrastructure". It's used for business development and networking to such a level that it's unthinkable to remove yourself from the system—even if LinkedIn can't keep your data safe. And without the pressure of losing users, LinkedIn may have little financial incentive to clean up its security practices. Which leaves users in the position of having to trust that LinkedIn will learn from it's mistakes—a pretty shaky proposition given recent events.

There is a common refrain from hordes of industry lobbyists that cybersecurity should be left up to industry to define and implement and that legislation and regulation—read any legislation and any regulation—is anti-business and anti-growth. This argument usually continues by saying that we should trust industry because it knows best.

Part of this is sometimes true: industry does often know how to protect cyber assets. The problem is that it doesn't always implement common sense and common practice. In an age when even Facebook can't get it's IPO right, is it really any surprise to learn that a tech company has cut corners? And what about companies that use technology don't see it as the core of their business? The IT department of most companies is seen as a cost center, so even if it knows how to implement a complete cybersecurity plan, would it be surprising to hear that the plan wasn't followed to cut costs?

The bipartisan cybersecurity bill that is now before the Senate addresses these realities by proposing comprehensive guidelines for cybersecurity. It patches gaps and standardizes and streamlines requirements so that companies have an easier time figuring out what they should be doing to maintain their defenses. Far from imposing undue burdens on industry, by setting common sense standards it makes it easier for businesses to know what they are responsible in ensuring cybersecurity. It's not a complete answer, but it's a good start.

Richard Wheeler is a Truman Security Fellow.

GPS, a Weak Link in Cybersecurity?

in The Truman National Security Project
By Richard Wheeler July 13, 2012

The news last month that LightSquared, a company attempting to deliver broadband internet via satellite, had filed for bankruptcy, settled a long-simmering but little noticed debate with far-reaching impacts on militaries, governments, businesses—and plain old folks like you and me.

Why? Because the global positioning system—better known as GPS—industry feared that LightSquared's technology would interfere with the GPS signal, a service on which the world has become increasingly dependent but which it also takes almost completely taken for granted. The LIghtSquared decision a pretty big deal in and of itself—but it also opens a window into the larger debate on cyber security which is now being argued both inside the Beltway and around the world.

GPS has become a part of everyday life around the world. Because as many geographers like to say, everything happens somewhere. And while GPS may not be as important as the internet as a whole, but it is an essential part of systems that effect every part of our lives. It's used by almost every component of the shipping industry that connects the planet, whether it be on land, at sea, or in the air. It's used in sensors and machines that monitor the weather and the environment. And it's used by you and me when we need to go to a new grocery store. It connects us to the physical world in a way we've never been connected before. If the United

Nations has declared the internet a human right, could they declare GPS a human right, too?

They could certainly try, except that it's a system that is entirely run by the United States military (there are similar systems to GPS, but nothing that has the same coverage). GPS was originally designed to help the military keep track of where it's service members and equipment is, and where to target weapons, and not where to find a Chipotle when you're hungry for a burrito. So as much as GPS is used all over the world for so many things, it's also a piece of America's critical infrastructure. Like the power grid, or communications networks, or gas pipelines, or interstate highways. So the United States government, along with the GPS industry, take strong steps to protect the system, both in terms of its physical and digital infrastructure and also the legislative and regulatory environment that makes it possible.

Sadly, industry that represents other critical infrastructures in America frequently resists efforts to shore up cyber defenses. The arguments trotted out by industry flacks frequently follow the party line that cyber defense cuts into the bottom line, which stifles growth and innovation. Even in the light of recent cyber attacks against Iranian oil industry, much of the United States' business community still thinks that it doesn't need comprehensive guidelines to direct cybersecurity efforts.

Here's the problem with that argument. Two of the most powerful organizations in America have already been hacked again and again: the United States military, and Google. And if the military and Google can be hacked, then how can anyone honestly believe that their business can't be hacked, too?

The LightSquared case shows us that in order to stay safe we need to look at comprehensive views of our infrastructure and its vulnerabilities. With LightSquared, the government deemed that the risk that its experimental technology could interfere with a critical system like GPS was deemed too great to allow the project to go forward. By a similar token, shouldn't it be reasonable for the government to create guidelines that help companies know what cybersecurity best practices they should follow? If wouldn't want experimental technology to threaten GPS, why would we let experimental or incomplete security technology threaten critical energy, transportation, or communications systems?

Something to consider next time you search GoogleMaps on your smart phone for "burritos."

Richard Wheeler is a Truman Fellow.

Securing American Business

in The Truman National Security Project
By Richard Wheeler June 27, 2012

As the debate on the future of cybersecurity in America continues to heat up, I'd like to take a moment to address one of the critical cybersecurity issues facing our country today:

My mother just bought a smart phone.

Why? Because they are new, and someone else she knows has one, and this person recently asked her if she sends text messages, and apparently this kind of peer pressure works at any age. And also because there was a sale at the Verizon store and like most Americans my mother can't resist a sale. So despite the fact that my mother had gotten by perfectly well on a 200 minute a month senior plan on a "dumb" phone, she upgraded.

And that's when the questions started.

"Richard, what is texting?" "Richard, how many minutes do I use when I send an email?" "Richard, why do I need a password on my phone?"

The list goes on, I assure you. They aren't bad questions, really. But they just start at such a basic level that explaining all of it gets a little exhausting. It's like trying to explain sex to a five year old. Or fractions.

Now I imagine you are thinking that this is all just because my mother is of a certain age, and that folks who grew up with technology—the so called digital natives—know how all this technology works as a matter of course. Digital natives, you might go on thinking, know the internet works, know what is safe and what isn't, and because of all this they make rational choices about their activity on the internet. And since these digital natives also run much of the internet, they most also make sure that all the companies they work for make rational choices about their activity on the internet.

And if you are thinking these things then you are 100% wrong—and what is wrong about what you are thinking is a critical point that is missing from the current cybersecurity debate.

Because people aren't rational. People are like my mom. They are swayed by emotion. They get distracted. They jump into things that they don't really understand. They are, in a word, people. There's nothing wrong with that. And there's nothing wrong with believing that people will make good choices, and hoping for the best.

But hope isn't a plan. And so sometimes we agree that we'd like a few rules here and there to make sure that people don't get a little crazy and forget what they are supposed to be doing. Remember when those pilots got distracted by their laptops and almost forgot to land the plane? Well after that the FAA made rules about using computers in the cockpit. Which hasn't stopped pilots from putting charts on iPads and using those to lighten their load while having more information at their fingertips, but has made it harder for pilots to get distracted by their emails (or Angry Birds). The bottom line is that some rules clearly make sense here, and rules don't by definition restrict innovation or growth.

We need to use the same kind of thinking when we think about the cybersecurity legislation now in Congress. A few common sense guidelines that require industry in critical areas to follow basic cybersecurity best practices is not going to cripple our economy or put Americans out of work, but they are going to make sure that we have a better chance of defending out critical infrastructure from cyber attack. We do need to nudge some companies a little to remind them what they should be doing, and if we do we'll all benefit.

Like with my mom's smart phone. It took me three tries to get my mom to put a password on it, but she finally did. Don't you feel safer already?

Richard Wheeler is a Truman Security Fellow.

Climate Studies Show: Somali Pirates Take Summer Vacations, Too
in WIRED's Danger Room
By Richard Wheeler June 25, 2012 12:00 PM

Somali pirates captured. Photo: European Union Naval Force

It's the first full week of summer, and most of us are probably thinking about how to get away to escape the heat, relax, and maybe hit a wave or two. Well, it turns out that Somali pirates take a summer break, too — but for different reasons.

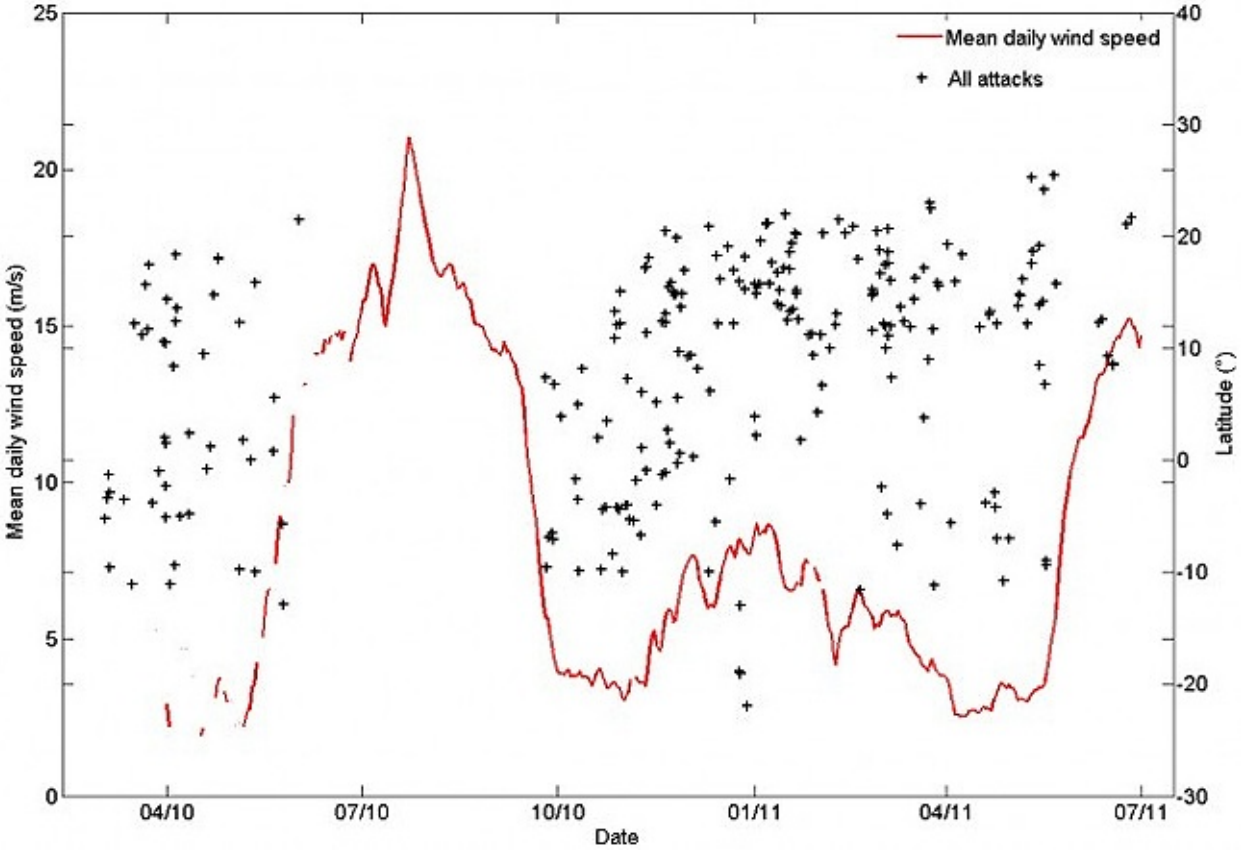
A recent report produced by researchers of the New Zealand Defense Force and the Royal Australian Navy (Climatic controls on piracy in the Horn of Africa region, 2010–2011) proposes a new spin on the observed temporal pattern of attacks by Somali pirates based on weather, or more specifically the monsoons that occur in the Indian Ocean and the Arabian Sea during the summer and winter.

Unlike previous reporting, which proposed that both summer and winter monsoons reduced pirate attacks, Climate Controls on Piracy finds that only the summer monsoon has a measurable effect on attacks. And unlike earlier analysis, which mostly took for granted the height of seas and force of winds during the monsoons, the new report uses data from European Space Agency environmental monitoring satellites. The researchers found that while waves and wind during

the winter monsoon was roughly twice that of non-monsoon months, this was not enough to deter pirates from operating in the Indian Ocean.

While this research doesn't provide a full picture of weather effects on pirate activity (for example, it does not address the possible shift of activity from the Indian Ocean to the Gulf of Aden and the Red Sea during monsoon season), it does indicate that in the summer Somali pirates are more likely to be found either in the confined waters of the Gulf of Aden or in their home bases in Somalia.

Which could mean bad news for you if you're a Somali pirate.



Mean daily wind speed at Socotra (Yemen) and pirate attacks by latitude for April 2010 to July 2011. When the wind speed dropped, pirate attacks increased. Courtesy of European Space Agency

It turns out that while the ocean is big, the coast that borders it is a lot smaller in comparison. Similarly, there are a lot of days in the year, but there are some that people are pretty sure to be at home. And there's a pretty easy to figure Venn diagram of when Somali pirates are pretty sure to be at home on the coast. Here's a hint: It's right now.

Last month marked the first attack by European Union Naval Force (EU NAVFOR) Somalia's Operation Atalanta on the Somali mainland. Although the nationality of forces involved wasn't released, a good guess is that they were French. The current Force Commander,

"responsible for the planning, orchestration, and execution of military activities", Rear-Admiral Jean Baptise Dupuis, is French. France typically contributes more ships to the force than other EU nations. The French Navy has more helicopters available than other navies participating in the operation, and France has a longer history of operations in Africa. And one more thing, despite typical American jokes to the contrary, the French have no hesitation in using military force.

But the EU as a whole is still trying to find its place as a military entity, both on its own and as a part of NATO, as evidenced by the uncertainty about how to conduct operations in Libya last year. So the successful attack in Somalia, which resulted in no European casualties and hit a universally despised and unambiguously clear target, might well prove a template for future attacks. Combine that with the news that pirates are likely to be home over the summer, and you shouldn't be surprised to hear about more land strikes soon.

So if you're vacationing in Somalia this summer and you hear someone yelling "Waxaa na haysto mashaakil!" you'll know it's time to get off the beach — fast.

Cyber Sensibility

in The Truman National Security Project
By Richard Wheeler June 15, 2012

While in-the-loop intelligence and defense insiders have been preaching about the dangers of cyberwar for more than a decade (think Richard Clarke) most of the world is just starting to catch up.

And they are scared.

Because even though it's great to think about cyberwar when you might be on the winning side (Stuxnet? What's a Stuxnet?), it's terrifying when you might be on the losing side (which is maybe why Iran has reportedly taken some of its oil terminals from the internet in the wake of a possible cyberattack). And the problem is that no one seems to know if they are winning or losing.

A major reason for this is that cyberattack, cyberwar, cybercrime—cybereverything—have taken on the character of a modern day Frankenstein monster. This thing called the internet has

gotten out of hand, and just like Peter Boyle in Young Frankenstein, once it's done tap dancing we want to hunt it down with pitchforks.

Many forget that the complete title of Mary Shelley's classic is Frankenstein; or, The Modern Prometheus, or the reason that Shelley referenced the classic Greek myth (similarly, many don't know why this is the title of Ridley Scott's new movie; so read on and you will instantly be the smartest person in your next water cooler chat/bar trivia contest/dinner party conversation).

The gist for all of you who didn't get a copy of a book on Greek myths from your parents growing up: Prometheus, a too-clever human tricks the gods and steals fire from them, and for this is punished by being chained to a rock where a giant bird visits him every day and plucks out his liver. Moral of the story: even if something is useful or really cool (for some the jury remains out on which of these best describes fire), there are some things that the gods are going to punish humans for having.

Like Facebook.

So what are we supposed do now that everyone has caught up the folks that were howling in the wilderness about the cyber threat, when we have become so dependent on the internet to maintain our infrastructure, create jobs, fight wars, and play Words With Friends? How can we keep the benefits of technology without risking the wrath of the gods? Or in less poetic terms, where should we direct our resources to build cyberdefenses and protect ourselves against cyberattack?

The answer of the day seems to be to make bigger and better Frankenstein monsters. In other words, to treat this as a technical problem that demands technical solutions and to take the human out of the loop. This is the answer that is and is going to be the favorite of many IT departments, software manufacturers, defense contractors, think tank wonks, and defense types. Each have their own reasons, and many of these—though not all—are well meaning. And we certainly do need to spend some resources on technology.

But where we need to start spending resources is on people.

We need to educate. This means efforts by industry to educate consumers about web tracking and targeted advertising. This means efforts by employers to educate employees about using computer systems safely at work and at home. This means efforts by schools at all levels to educate students on what is safe, and what isn't, on the internet.

We need to make computer users more aware of cyber threats and also demystify them. Because as much as many tech professionals would like to remove the human from the system, the fact is that everything in our world is pushing more and more people onto the web more and more of the time.

If we continue to live in a world where the most common password on computer systems is

"password" then we have indeed created a Frankenstein monster, or in the context of the Prometheus myth, we have found a power which we will be punished for playing with. The difference between these stories and the reality of cyberwar is that we may still have the ability to learn to stop our own destruction, if only we learn to do so.

Richard Wheeler is a Truman Security Fellow. He is a designer, a writer, and an analyst. He likes maps. He likes pictures. He likes to figure out how things work.

"Chaff": A continuing project to not be found

By Richard U. Wheeler
Saturday, June 9, 2012 at 06:34PM

For a number of years now I have engaged in various (mostly futile) strategies to maintain my privacy and anonymity on the internet. These continue as semi-serious projects, but are also things I would like to develop further as art pieces.

The latest iteration of these projects is a Facebook project loosely titled "Chaff". Chaff in this sense not just being the stuff you have to wade through to get to wheat, but also the term for a kind of active countermeasure developed in the Second World War to confuse radar.

In this iteration of the project, every month I perform the following actions:

1) I generate 20 random two word phrases (adjective, noun) using http://watchout4snakes.com/CreativityTools/RandomWord/RandomPhrase.aspx
2) I enter each phrase into Google Image Search http://www.google.com/imghp?hl=en&tab=wi
3 I download the first image that comes up in search (or in some cases a funny image from the first page of results)
4) I upload the resulting 20 images to Facebook
5) I tag each image as myself

The intent of this is to jam Facebook's facial recognition algorithms with so much bad data that they are unable to detect pictures of me on Facebook or elsewhere. Or at least make that process a lot harder.

A few results from my latest round follow.


Goldfish
Wet Ones


ROAD TRIP
KIT
3 Little Trees


手軽に一品
家庭の味。
煮物の具
大根の小鉢
小鉢で
約6人前


FX


CHARLTON COMICS
BLUE BEETLE
12¢
NO.3
OCT.
APPROVED BY THE COMICS CODE AUTHORITY
CDC
THE MOOD IS MADNESS WHEN THE BLUE BEETLE MIXES IT WITH THE MADMEN!
KZZZZZZZ
RETAILERS: SEE PAGE 28 FOR SPECIAL DISPLAY ALLOWANCE PLAN


Henry Stimson

Groundtruthing: "Points of Interest"; Part II

Richard U Wheeler
Saturday, June 9, 2012 at 06:30PM

I have continued to explore Southern California and document the sometimes strange and often banal places both frequently and rarely photographed from space.

The results of my recent travels follow.

Riverside County: High

Riverside County: Low

San Bernardino County: High

San Bernardino County: Low

Kern County: High

Kern County: Low

Groundtruthing: "Points of Interest"; Part I

Richard U. Wheeler
Monday, March 12, 2012 at 08:04PM

Using data from the analysis I conducted in December and January I have set out over the past two months to begin to document some of the spaces I have identified as both areas of high commercial satellite imagery collection and low commercial satellite imagery collection.

Why? To paraphrase Sir Edmund Hilary, because I want to know what is there.

For each county in southern California I identified these areas of high and low collection. For each of these areas I then identified the center—or rather what is called the centroid, which is a technical term for "approximately the center," "sort of the center," or "center-ish." For each of these points I determined its geographic coordinates, and then checked them on a map, hopped in my car, plugged the coordinates into my GPS and drove out to find what was there.

The results are both predictable and surprising. These are a selection, though not necessarily the final set.

Los Angeles County: High

Los Angeles County: Low

Orange County: High

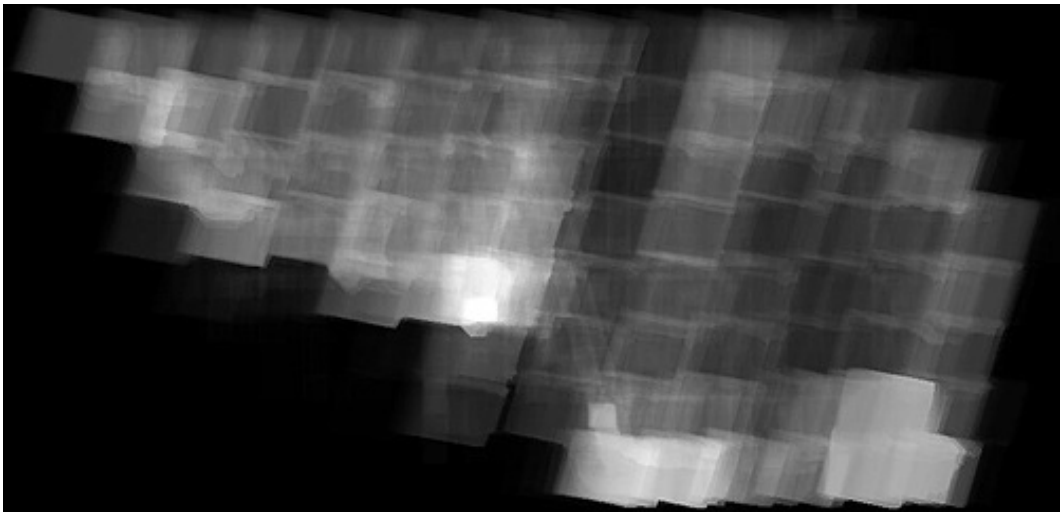
Orange County: Low

Ventura County: High

Ventura County: Low

Analysis: "Points of Interest"

Richard U. Wheeler
Tuesday, January 17, 2012 at 05:43PM



[The field of view is of Southern California]

On February 22, 1986, the first commercial satellite, SPOT, was launched, and two days later on February 24, 1986, it began transmitting images back to Earth, and so began a new era in the long history of surveillance from the skies. What was once only available to only the most powerful militaries was now a commercial product available to businesses, to academics, and even to the public. While the number of images was initially a trickle, over the years more satellites were launched, more companies entered the market, and eventually the trickle became a flood. In a single generation we have moved from a world where space imagery, or aerial imagery of any kind, was rare and exotic, to a world where you can pull up a relatively recent image from space on your phone.

Not surprisingly, satellite imagery focuses on population centers, or on areas that are important in the news. Some companies use a standard collection plan, and others collect on a more ad hoc basis as a result of customer requests. There is not one business model for commercial satellite imagery production, there is no centralized requirements list that drives commercial satellite imagery collection, and there is no central repository for these images. As far as commercial satellite production is concerned it is still a little wild, wild west in the cold reaches of near Earth orbit.

An unintended result of this competition is that for any given region on Earth, the location of maximum and minimum collection is totally unintentional. I will explain this more fully in a later post, but essentially it works out as follows: since there is no coordination between providers or clients, the location of images in time and space overlap in random and unintended ways.

The image above is the beginning of an exploration into where these unintended places are

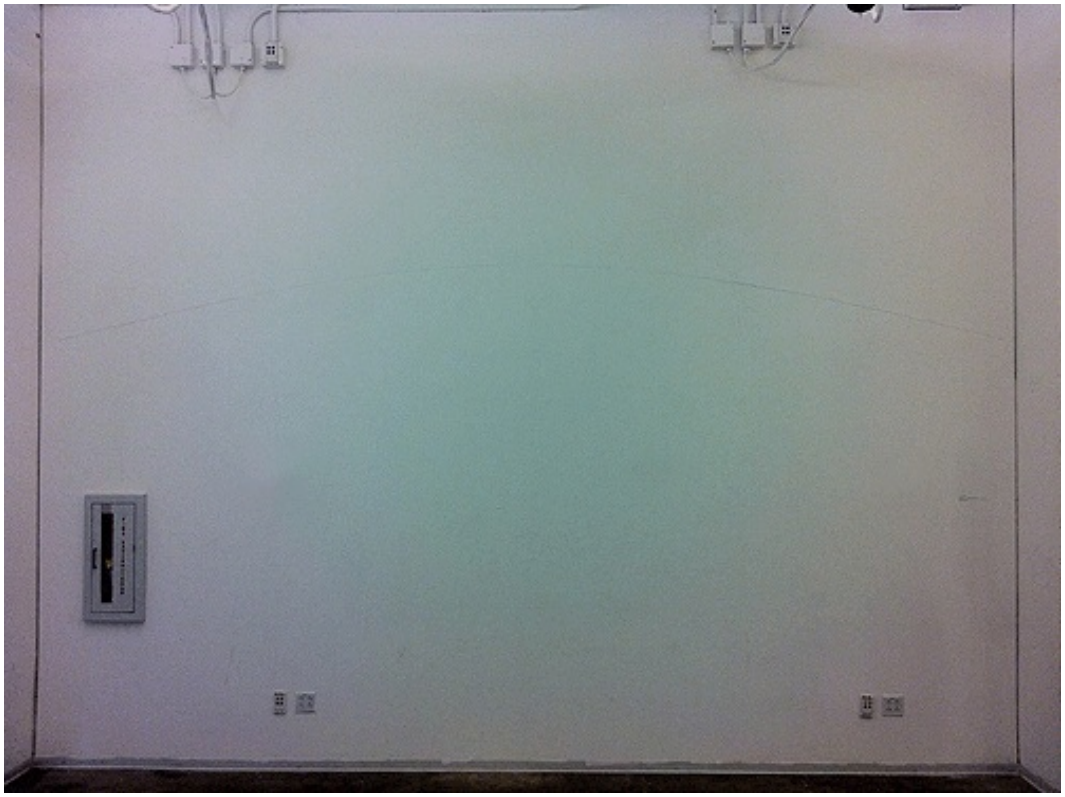
located, and into what is there. It is not a representation of images themselves but rather of their location, or what is often called their footprint. The image represents the overlaps of 49,141 images taken in the first 25 years of commercial satellite imagery, from the satellites operated by Astrium (SPOT 1-5, KOMPSAT-2), Digital Globe (QuickBird, WorldView-1, and WorldView-2), and GeoEye (GeoEye-1, and IKONOS). I'll get into the rationale behind this list in a later post, along with alternative lists. No matter how you look at it though, this dataset is a pretty good start. Because of the limitations that I had on processing power and time this image was created by converting each footprint, which is essentially an outline, into a grid of pixels, or also know as a raster, and then adding all of these pixels together. Again, more on this later.

The result is an image where the light areas represent areas on the Earth that have been photographed many times and the dark areas represent areas on the Earth that have been photographed few times. As this project progresses I will be experimenting with different ways to visualize and interpret this dataset, but even in this raw form strange and interesting patterns begin to emerge. These kinds of effects nearly always happens with this kind of data analysis, and I will be exploring some of the followon effects of these anomalies later.

For now I invite you to explore and ponder this strange artifact of a quarter century of human exploration.

"For Alexandra on the eve of her 29th birthday..." A wall drawing

Richard U. Wheeler
Monday, December 5, 2011 at 03:25PM

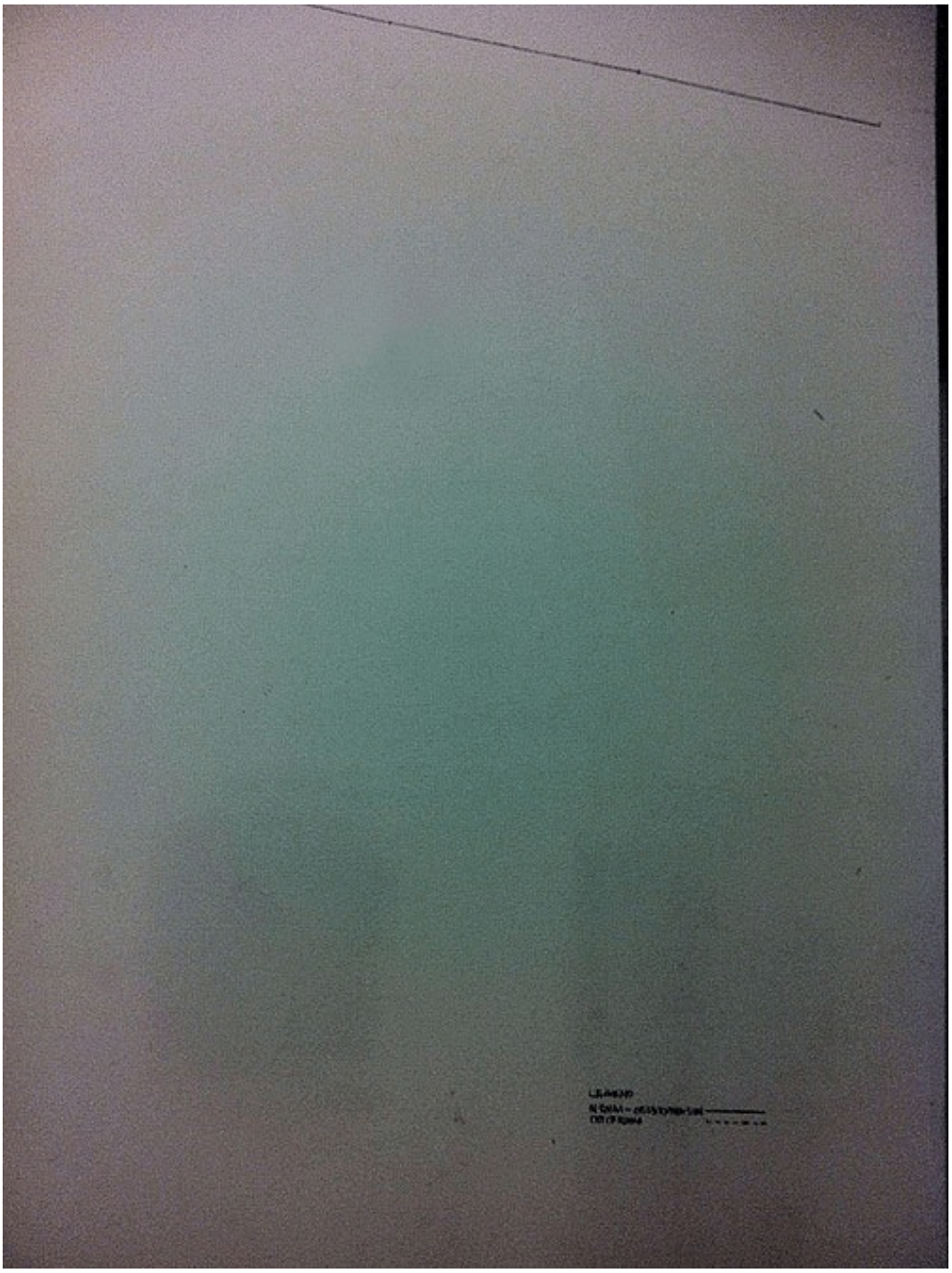


For Alexandra on the eve of her 29th birthday: The path of the sun projected onto the south wall of Room 2250K, Broad Art Center, UCLA, Los Angeles, California, United States of America, ~118°26'W 34°05'N, seen from a distance of about 90" from the wall, drawn in real time in 10 minute increments on December 4, 2011 from 1730 to 2200 GMT, interrupted by chance from 1830 to 2040 GMT. is a wall drawing I created at UCLA's Design | Media Arts Program.

I used data from the United States Naval Observatory (USNO) to plot the location of the sun as it would been seen from 118°26'W 34°05'N on December 4, 2011. I combined this data with measurements of the geometry of Room 2250K, Broad Art Center, UCLA and used a bit of homebrewed analytics to project the path of the sun onto the south wall of the room. I then drew this path in real time in 10 minute increments — in other words I drew a point every 10 minutes representing the position of the sun at that moment, and then connected these points to form the arc.

Although I intended to be in Room 2250K throughout the day on December 4, 2011, I was called away. This time is represented by a broken line in the arc.

This piece is a new direction in a path that I started down many years ago. It is a drawing that at the same time records, time, place, activity, and thought. I hope to do more soon.



""TYPICAL" CLOTHING UCLA NORTH CAMPUS SITE 20111011 1020-1100GMT+7"

Richard U. Wheeler

Tuesday, October 25, 2011 at 03:45PM

"TYPICAL" CLOTHING UCLA NORTH CAMPUS SITE 20111011 1020-1100GMT+7 is the first in a series of projects I am creating at UCLA's Design | Media Arts Program that combines a number of personal and professional interests, including surveillance, image processing, and personal presentation.

The brief for the project:

> Set up a surveillance site in a public area. Observe male pedestrians. Review the images and classify what clothing the persons in each image are wearing. Analyze the resulting classification notes and determine what is the typical clothing for this location.

Blowup of first two pictures of Typical Clothes .pdf file.

||20111011|1020|1100|GMT+7|001|upperBody.2.type:Shirt|upperBody.2.fit:Regular|upperBody.2.sleeve:Short-sleeved|upperBody.2.front:Full-button-front|upperBody.2.neck:Collared|upperBody.2.color1:White|lowerBody.1.type:Pants|lowerBody.1.style:Trousers|lowerBody.1.fit:Regular|lowerBody.1.leg:Full-leg|lowerBody.1.hem:Plain|lowerBody.1.color1:Black/blue-dark|foot.1.type:Dress-type|foot.1.fit:Low|foot.1.color1:Black|bag.1.type:Shopping-bag-plastic|bag.1.size:Small|bag.1.color1:White|bag.1.carried:Right-hand|other.1:"Sweater, carried in left arm"|||

||20111011|1020|1100|GMT+7|009|upperBody.3.type:T-shirt|upperBody.3.fit:Regular|upperBody.3.sleeve:Short-sleeved|upperBody.3.front:Pull-over|upperBody.3.neck:Unknown|upperBody.3.color1:Black/blue-dark|lowerBody.1.type:Shorts|lowerBody.1.style:Unknown|lowerBody.1.fit:Regular|lowerBody.1.leg:Knee|lowerBody.1.hem:Plain|lowerBody.1.color1:Grey-dark|foot.1.type:Sandals-unknown-type|foot.1.color1:Black|bag.1.type:Backpack-Northface-type|bag.1.size:Medium|bag.1.color1:Black|bag.1.carried:Back|||

Richard U. Wheeler

I've started a new adventure: a MFA program in Design and Media Arts at UCLA!

Wednesday, September 21, 2011 at 03:54PM

After nearly four interesting and fruitful years at Esri, I have decided to spend a little time back in academia in UCLA's Design | Media Arts Department. I'm pursuing a Master's in Fine Arts degree, and I'm going to be studying how design and technology can interest to create both fine art and design solutions to a range of real-world challenges.

Check this space for more work as it develops.

How to Talk Like a Pirate … in His Native Somali

in WIRED's Danger Room
By Richard Wheeler
September 19, 2011 2:00 PM

Sept. 19 is International Talk Like A Pirate Day. For most would-be buccaneers, this is an opportunity to drink grog and try out their best Captain Jack Sparrow impersonations. Danger Room certainly does not discourage this kind of behavior.

At the same time, piracy is not just a thing of the past, but rather a real-world problem plaguing the some of the most dangerous areas of the world today. And so with this in mind but also in the spirit of International Talk Like A Pirate Day, Danger Room would like to offer this guide to talking like a real pirate — as in, the one of the guys hijacking ships in the Horn of Africa region today. It's the first in what may become a series of ITLAPD features.

The Horn of Africa is without question the hotbed of piracy today. A quick glance at the International Maritime Bureau's Piracy Reporting Centre Live Piracy Map shows a dense thicket of attacks, and even though some analysis indicates that the areas of attacks may be decreasing in size, and that the frequency of successful attacks is decreasing, the density of attack is increasing and the risk of attacks remains high . And the focus of this activity remains Somalia.

What languages are these pirates speaking? Based on the IMB's reported risk zones, and country data for Somalia from the CIA's World Factbook, they are probably speaking in Somali, Arabic (probably a Yemeni dialect), Italian (a vestige of Somalia's colonial heritage) or English.

But what exactly are they saying? A good source for how to say something important in a combat situation at sea – and in a host of other interesting situations – are the Defense Language Institute's Field Support Modules for a given language. Sadly, Danger Room can't help you out dealing with pirates on your next trip to Lake Como as DLI does not produce an Italian module, but below are 20 common pirate phrases in English, Somali, and Yemeni Arabic, along with where you can find them in the guides.

	Guide	Section	Phrase	English	Somali Transliteration	Somali	Yemeni Transliteration	Yemeni
1	Navy	Bridge Commands	01-03	Where is the control room?	roogta hoganka?	rugta hogaanka?	feyn ghurfat attaHakum?	فين غرفة الـ تحكم؟
2	Navy	Bridge Commands	01-11	Stop the engines!	matorka demee!	matoorka demi!	agif al-muHarikaat!	وجف! المحركات
3	Navy	Bridge Commands	01-01	Where is the captain?	damehee meyay?	dhammehii meeyay?	feyn ar-rubaan?	فين الربان؟؟
4	Navy	Prisoner Questions	09-15	Who is the captain?	damaha waa key?	dhammaha waa kee?	man hoo ar-rubaan?	هو مَنْ الربان
5	Navy	Bridge Commands	01-05	How many men are on this ship?	imisaa qof baa saran markabka?	imissa qof baa saran markabkan?	kam beh reejaal bilmarkab?	رجال به كم بـ المركب؟
6	Navy	Questions and Needs	08-02	Do you have weapons?	hoob meeyaad haysataa?	hub miyaad hasataa?	beh 'indakum asleeHa?	عندكم به أسلحة؟
7	Navy	Bridge Commands	01-02	Where are the weapons?	hoobkaagee meyay?	hubkaagii meeyay?	feyn al-asleeHa?	فين الأسلحة؟
8	Navy	Critical	03-02	Do not	ha naga hor	ha nnaga	maa	ما جاوش!

		Commands		resist!	imaaneen!	hor imanin!	tigaawimsh!	
9	Navy	Critical Commands	03-14	Don't move!	ha daqaaqin!	ha dhaqaaqin!	maa tit-Haraksh!	ما تحركش!
10	Navy	Critical Commands	03-15	Come here!	halkan imo!	halkan imoow!	jee laa haanaa!	هنا لا جي!
11	Navy	Critical Commands	03-18	Hands up!	ga'maha kor oo qaad!	gacmaha kor u qaad!	irfa' yadaatak!	إرفعْ إيدا تك!
12	Navy	Critical Commands	03-23	Don't look at me!	ha ee so feereen!	ha i soo fiirinin!	maa titfarajsh lee!	ما تتفرجش إلي!
13	Navy	Critical Commands	03-03	Look forward!	horey feeree!	horay fiiri!	ibSir gudaam!	إبصر إجدام!
14	Navy	Critical Commands	03-04	Close your eyes!	indahaaga Hir!	indhahaaga xir!	banid 'ayoonak!	ع يونك بَنِّدْ!
15	Navy	Critical Commands	03-07	Kneel!	jilbaha doolka dig!	jilbaha dhulka dhig!	irka' 'ala rukbatak!	عـلى إركعْ ركـ بـ تك!
16	Navy	Critical Commands	03-12	Hands behind your head!	ga'maha madaHa saar!	gacmaha madaxa saar!	Dha' yadatak waraa raasak!	يـ داتـ ك ضعْ وراء رأ سك!
17	Aircrew	Emergency Transmissions	01-02	We have a problem.	waHaa na haysta mashaakil	waxaa na haysto mashaakil	beh 'endana mashkeela	عـندنـا بـه مـشـكـلة
18	Basic	Commands, Warnings and Instructions	01-01	Stop!	jogso!	joogso!	ogaf!	أوجفْ!
19	Basic	Commands, Warnings and Instructions	01-02	Stop or I will shoot.	eestag ama waan koo toganaya	istaag ama waan ku tooganayaa	ogaf wila aTlagt 'aleyk an-naar!	وإلا أوجَفْ أطـلجت عـلـيك الـ نار!
20	Basic	Commands, Warnings and Instructions	01-23	Surrender	is deep	is dhiib	salim nafsak	نـ فـسك سَلِمْ

Photo: Wikimedia; chart: Richard Wheeler

Here's How U.S. Spies Will Find You Through Your Pics
in WIRED's Danger Room
By Richard Wheeler
July 29, 2011 7:00 AM

Iarpa, the intelligence community's way-out research shop, wants to know where you took that vacation picture over the Fourth of July. It wants to know where you took that snapshot with your friends when you were at that New Year's Eve party. Oh yeah, and if you happen to be a terrorist and you took a photo with some of your buddies while prepping for a raid, the agency definitely wants to know where you took that picture — and it's looking for ideas to help figure it out.

In an announcement for its new "Finder" program, the agency says that it is looking for ways to geolocate (a fancy word for "locate" that implies having coordinates for a place) images by extracting data from the images themselves and using this to make guesses about where they were taken.

More and more digital cameras today don't just take pictures but also capture what is called metadata — often referred to as data about data — that can include everything from when the picture was taken to what kind of camera was used to where the it was taken. This metadata, often stored in a format called EXIF, can be used by different programs to understand different

aspects of the image — and also by intelligence analysts to understand different aspects of the user who took it, and the people who are in it. Like who they are, what they are doing, and where and when they did it.

Sounds great! But there are a few small problems.

First, not all images are digital. Those old pictures of your parents that you scanned? No metadata. Also, not all digital image formats support metadata. That BMP file you've got from 1996? No metadata there, either. Next, even if the image format supports metadata, not all digital images are captured with it. Or they are, but they aren't captured with a full set. That picture from your old-model Flip phone? No metadata there, or not enough metadata. Also, many popular websites — for example Facebook — strip EXIF tags. So it's not possible to get the metadata unless you can somehow get access to the source file — which means hacking.

All that means that there are a lot of images out there with no metadata and/or with metadata that you can't get to very easily. But these images might still have visual information within the image, or other clues, that could enable a system — either completely automated or using automated and human processes together — to make a guess about where the image was taken. The best case for intelligence analysts would be a fully automated system. This way they could suck in images from a terrorist website, download them off of captured cameras or cell phones, or scan them from hard copy, and feed all this through the system and get locations of where the images were taken. With more and more images being created in our world every day this automated approach is going to be crucial.

You can already see a little bit of this happening with the new Google Image Search. The new Google Image Search has a "reverse image search" capability that enables you to search for other instances of the same image on the web. In most cases, this is limited to the exact same image. For example, open up Google Image Search into a second browser window and drag in this image:

No matches. So is this helicopter flying over Khost Province in Afghanistan or flying over the back side of the Hollywood sign? Hard to tell from the image itself. And if you test out typing both "Khost Province" and "Hollywood" into the search bar, you'll get results that point in both directions. Even for a trained human analyst, this might prove too hard to crack (although the lack of rocket pods on this helicopter makes a good case for this not being an MH-6 Little Bird, which points to Hollywood over Khost).

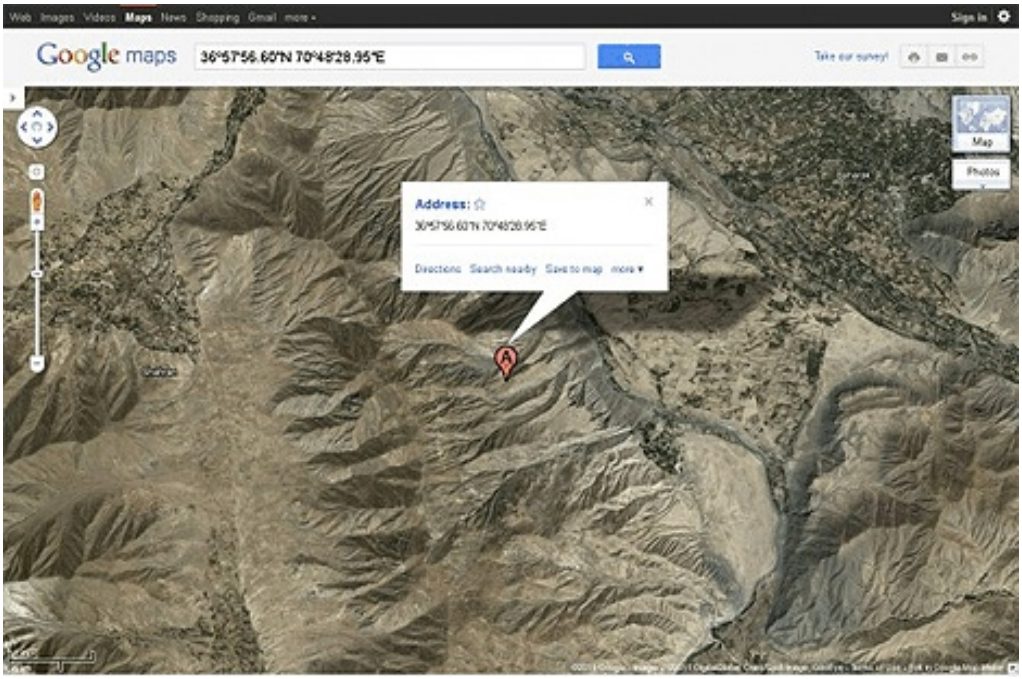
But for some places that have been photographed over and over again, Google can guess where the image was taken. Drag this into Image Search:

If you didn't guess already, or if you're still figuring out Image Search, or if you're impatient, or if you're just lazy, here's a hint: It's the Grand Canyon. Not too hard for Google to guess because so many people have shot it. When it works like this, Google Image Search is almost like a biometrics program for places.

There is also a middle ground where there will probably still be a place for the human, probably with the images that also have some text data associated with them, where skills of not just pattern matching but intuition will be useful.

The caption for this image reads "An Mi-17 helicopter flies to Kabul, coming back from a

humanitarian assistance mission in Baharak, Badakhshan province, Afghanistan." If you didn't know it was Afghanistan you might think you were looking at the Sierras, but once you know it's Afghanistan, and Badakshan province, and near Baharak, and taken on a flight from Baharak to Kabul, and you take a look at the big peak in the background and the distinctive runoff pattern in the foothill at the bottom of the frame, a trained analyst might be able to poke around in a 3D visualization program like GoogleEarth and say that the picture was taken around here:



Iarpa will

probably look for combinations of both of these approaches, but on an industrial scale. It's a hard problem, but even now we are starting to see the beginnings of the solution even in the commercial world. And you better believe that it's not just spooks who want to know where images were taken. Google, Facebook, Apple and all the other internet and social media giants are probably looking to do the same thing so that they can better understand where their users are and what they are doing there.

So before long your Facebook or Google+ account will be automatically tagging who is in your pictures and where they were taken…

…and spooks might be, too.

Photos: 55th Combat Camera, U.S. Army; Richard Wheeler; Jonathan Zander/CC; 438th Air Expeditionary Wing, USAF; Google, Cnes/Spot, DigitalGlobe, Europa Technologies; Google, Digital Globe, Cnes/Spot, GeoEye

"Gone (spear)-phishing..."
Saturday, July 2, 2011 at 01:13AM
Richard U Wheeler in cyber

If you're a United States military service member — or maybe even if you just follow defense news — get ready to be spear-phished.

Again.

On June 27 Gannett Government Media — a subsidiary of media giant Gannett that publishes a range of defense and intelligence focused publications including Army, Air Force, Navy, and Marine Corps "Times", the Armed Forces Journal, and Defense News — announced that on June 7 it had suffered a cyber attack where information on some users had been accessed, including "first and last name, userID, password, email address, the internal number we assigned to the account, and, if provided, ZIP code, duty status, paygrade, and branch of service."

In some ways the Gannett attack is just the latest in a recent rash of intrusions, including:

On May 10 Citigroup was attacked and the "…customer names, account numbers and contact information…" of more than 360,000 credit card holders was accessed.
In mid-April the Sony PlayStation Network was hacked and the "…names, birthdates, physical and e-mail addresses, and PlayStation Network/Qriocity passwords, logins, handles and online IDs" of the service's 70 million users were potentially compromised.
On March 30 an attack on Epsilon, a firm that sends marketing emails for more than 2,500 companies to millions of recipients, accessed records for 19 firms containing users names and emails.

In each of these cases, and in previous ones, security experts warned of spear-phishing in their wake. Spear-phishing is the computer security term for targeted phishing attacks. "Phishing attacks work by the scam artist sending 'spoofed' emails that appear to come from a legitimate website that you have online dealings with such as a bank, credit card company or ISP — any site which requires users to have a personal identity or account. The email may ask you to reply with your account details in order to 'update security' or for some other reason." Unlike traditional phishing attacks, which are usually blasted out with little personalization, spear-phishing is customized to the target, often containing personal information and other details that might increase the target's willingness to trust the authenticity of the sender and then usually either click through to a website that will download malicious code onto the users machine or download a file containing malicious code.

But what makes the Gannett attack different is the fact that it was targeted at individuals in the military (although the same could be said of more than a few of the users of the PlayStation Network). Although not all readers of Gannett Government Media's publications are military service members, many are, and their ZIP code, duty status, paygrade and branch of service information in Gannett's database represents a treasure-trove for potential spear-phishers.

Less than a month ago, Google uncovered a spear-phishing attack directed against personal accounts of "senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists." While this attack specifically targeted senior level officials, previous attacks directed at military personal have not necessarily been segregated by paygrade. And one of the lessons of the Bradley Manning/Wikileaks incident is that sometimes an E-4 can have access to more information than an O-4 — and maybe give less thought to how he or she uses it.

The March attack on RSA Security, a leading security firm that supplies government, military and defense contractor organizations with authentication tools, led to spear-phishing attacks on defense contractors Lockheed Martin and L-3 Communications less than a month later. By waiting 20 days to release news of the attack on their systems, Gannett has given would-be attackers plenty of time to prepare a similar assault. Sony has already taken criticism from private sector security experts and from Congressional committees for its lag in releasing news of the PlayStation Network breach, and Gannett may come under similar criticism from the same corners. But another question that comes out of this incident is if, and how, businesses and organizations that serve military service members should protect user data, and if there are any additional precautions that they should take with this data.

The US Department of Defense has struggled in the past few years to cope with the rapidly changing pace of information technology, stumbling over issues as varied as social networking to thumb drives as it tries to balance the needs of its service members to stay connected in a digital world against the threat of attacks from both cyber criminals and cyber warriors. And while it can to some extent control what happens on DoD systems, the fact is that with so many service members deployed so often for so long, there is perhaps a greater threat in the vulnerabilities within the many commercial web services that services members use every day to stay connected to the world outside of the war zone. And while the government and private sector often come together to encourage best practices in coding web sites — for example the recent joint project of the Department of Homeland Security, the MITRE corporation, and the SANS Institute to identify the "…top 25 technical software problems that hackers exploit…" — there is still a long way to go in creating best practices for what user can should be stored, and how, and for how long. And while the government may not want to get involved in what seems like a private sector problem, unless there is a discussion about how to protect the identities and personal information of service members they are likely to be targeted for more frequent and more sophisticated attacks.

Again.

Did Two Profs Find Osama From Space? Nope, Sorry.
in WIRED's Danger Room
By Richard Wheeler
May 6, 2011 7:00 AM

Locating Osama bin Laden took years of painstaking intelligence collection and analysis . And despite what you see on 24, there is no magic. Each piece of the puzzle had to be fitted together over time, something that doesn't happen easily or automatically — especially when the intelligence is used to back a decision send people in on the ground instead of dropping a bomb or firing a cruise missile.

But the seemingly insatiable hunger for magic has popped up in the renewed slew of press coverage of a 2009 paper, "Finding Osama bin Laden: An Application of Biogeographic Theories and Satellite Imagery," by UCLA geography professors Thomas Gillespie and John Agnew. Typical headlines describing this paper include "Geographers Had Predicted Osama's Possible Whereabouts" and "This Class of Geography Students Found Bin Laden's Hideout Long Before the CIA."

These stories are simply wrong. By failing to describe what the paper actually says they both distort the real work that went into finding Osama bin Laden and cloud the question of how the techniques Gillespie and Agnew describe can be used in the future.

It's important to point out, as Danger Room did when the paper came out in February 2009, that the paper was an academic thought problem, and was not an actual mission to find Osama bin Laden. If the UCLA team was using their methodology to actually try and find bin Laden, they would have probably incorporated many of the criticisms I will outline, and may have gotten better results.

So, did the paper say that Osama bin Laden could be found in a compound built in Abbottābad, Pakistan?

No.

In fact, the paper said that the most likely location for bin Laden's hideout would be in Parachinar, a city about 268 kilometers away from Abbottābad.

Second, if the paper didn't say that bin Laden would be in Abbottābad, did the paper at least say that bin Laden was 88.9% likely to be there?

No.

In fact, the paper said that the likelihood that he would be somewhere within 300 kilometers of Tora Bora would be 88.9%.

Actually this was never spelled out, but you can derive it the from the formulas in the paper, where P(d) = 0.99959058977238d, d equals distance in kilometers, and P(d) is the probability that bin Laden could be within distance d from Tora Bora (Math is fun! Also, when I do the math I get 88.44%, but who's counting?).

If this seems like common sense, it should. One of the things that the distance decay model that the team used basically says is that when people (or animals, or plants) are on the move, you are more likely to find them closer to where you last saw them than farther away.

But even though Abbottābad falls within this area of 88.44% probability, so does Islamabad, Kabul, and numerous other urban areas. And the model doesn't give any indication of the likelihood that bin Laden in one of those places or any other point in the 282,743 or so square kilometers defined by the 300 kilometer radius circle whose center is at Tora Bora, only that he is 88.44% likely to be somewhere in that circle.

So Gillespie and Agnew did not claim that they knew where bin Laden was hiding in 2009, and they aren't now. What they were saying is that there might be ways to use tools of geographic analysis to try and predict where bin Laden might be. In 2009, Gillespie was quoted as saying, "we are all wondering where bin Laden is hiding," Gillespie says. "We just wanted to offer the techniques we have to help." That makes sense, but the question then becomes whether the techniques they offered can help.

They can, but not without some work.

First, the authors assume that there are equal travel costs to all points from Tora Bora, regardless of terrain, cultural geography, political geography, transportation networks, or other features. This simplifies the model but is unrealistic. The model would need to incorporate varying travel costs to be more useful.

And even though their model doesn't make assumptions about travel costs, the authors do, and they set a somewhat arbitrary limit of travel of 20 kilometers from Tora Bora over an eight year period. This assumption flies in the face of reality, and assumes that the most powerful terrorist leader on the planet could not get a little help from his friends. The model needs to deal with time and resources better to be more useful.

Once the authors isolated a large area of interest, they used Defense Meteorological Satellite Program Operational Linescan System imagery to isolate urban islands. This methodology measures nighttime lights, and basically says "the more light there is at a given point the more people there are likely to be at that point." Using this technique the authors identify 26 urban islands where bin Laden could be, and this more or less works. They then chose Parachinar from this list based on a set of assumptions — which turn out to be questionable.

For example the authors fail to take into account important cultural factors. A 2009 response to the paper by Murtaza Haider notes "Since I am from the Northwest Frontier Province, I find it a little odd that Osama [a Sunni Muslim] may be hiding in the only Shiite majority town in the entire tribal region of Pakistan." The lack of cultural awareness in the paper, and the consequent failure to realize that not all areas would be equally available to bin Laden as hiding spots, weakens the analysis considerably.

Finally, once they had narrowed down their search to Parachinar, the authors used high-resolution satellite imagery from Digital Globe's QuickBird satellite to perform manual imagery analysis of structures to assess whether they might be potential hideouts. But here at the last mile their methodology breaks down even further.

They score structures based on a profile of bin Laden's assumed "Life History Characteristics": "Each structure was quantified as 1 or 0 for accommodating each one of these six characteristics. Structure values were summed and the highest values (for example 5 or 6) were selected as his probable location." But many of their assumptions are either false or flawed.

For example, based on the characteristic "Is 6' 4" tall" the authors assume "Tall building." But tall people do not get tall buildings and short people do not get short buildings — all people usually get buildings that are about the same size. Next, the authors assume that bin Laden had kidney problems that required access to a dialysis machine. But as Danger Room's 2009 review points out, "the professors accept as fact that bin Laden requires a kidney dialysis machine. That means he must need to be close to an electrical grid or generator, the UCLA pair reason. Too bad the thing is complete folklore — debunked again and again."

There are flaws in most of the remaining four assumptions, and what this leads to is a high chance of the model producing false positives. Also, the work in this last step would require

hours of skilled human imagery analysis per candidate structure, which means that even to get to the 26 candidates in Parachinar it could take weeks of work — and remember that Parachinar isn't even close to Abbottābad.

These could be addressed and the model could be refined to produce better results. The authors note that "These methods are repeatable and could easily be updated with new information obtained from the US intelligence community on his last known location." As possible next steps following from their research the authors wrote that the National Security Agency, the National Geospatial Intelligence Agency, and the National Reconnaissance Agency "should also disprove the hypotheses that Osama bin Laden is: (1) located in the Kurram region of Pakistan, (2) located in the city of Parachinar, and (3) at one of the three hypothesized buildings."

But what they failed to realize is something that was proven out in bin Laden's takedown: none of these agencies could perform these tasks alone. They are all agencies that work remotely, and use technology to do so (and NRO isn't even really in the analysis business, which the authors miss). But the takedown Osama bin Laden took months of physical surveillance, human intelligence and finally 79 pairs of boots on the ground (and four paws) to assault the compound, kill its defenders, and kill bin Laden. If one had to repeat this process for every candidate turned up by the UCLA team's things would have gotten ugly. And they will get ugly if we rely on this kind of methodology going forward.

The kind of abstract, data-driven analysis that Gillespie and Agnew propose can be effective as a tool to direct human intelligence and operations, but only if it is combined with a knowledge of human geography. This is a critique that can partly be heard from reports penned by the Army's controversial Human Terrain project to Major General Michael Flynn's 2010 paper "Fixing Intelligence: A Blueprint For Making Intelligence Relevant in Afghanistan." But it can never be a substitute for ground truth knowledge and operations. The takedown of Osama bin Laden shows that despite our best technologies there is no magic to fight battles, only hard work.

Satellite image courtesy of GeoEye

If You Can Tell Boys From Girls, the Air Force May Give You 20 Grand

In WIRED's Danger Room
By Richard Wheeler
April 14, 2011 7:00 AM

Updated 8:57 am

The Air Force has problems distinguishing men from women and adults from children. Which means pilots sometimes target — and kill — the wrong people. The air service's solution: a nationwide contest, to help the military pick out kid from grown-up.

With the "Remote Human Demographic Characterization" challenge, the Air Force is looking for descriptions of a system "that can determine approximate age (adult, teen, child) and gender of small groups of people at a distance." The challenge "requires a written proposal only." So if your idea works and you can get the technical details right, you could walk away with $20,000.

The challenge is one of four that the Air Force Research Lab set up with the launch of its new Open Innovation Initiative. It attempts to use models pioneered by Darpa and NASA to use contests to find solutions to hard problems. Other current Air Force challenges include "Design and Simulation of an Accurate Shooter-Locator" for a whopping $50,000 and "Humanitarian Air Drop" for $20,000.

In light of recent reports indicating that the first drone friendly-fire incident may have occurred in

Afghanistan, the military will certainly be taking a hard look at how drone surveillance operators are identifying targets and authorizing attacks. U.S. forces usually wear special infrared reflective patches on their uniforms that could have alerted the Predator operators in this incident that they were looking at friendly forces, but these patches are small and might not have been viewable from all angles. And in a high-pressure situation with troops under hostile fire, the Predator operators could well have felt pressure to attack, to support the troops on the ground.

But the issue that many drone operators are facing every day is different: how to pick out combatants from noncombatants in environments where there are no uniforms and where fighters mingle with freely with civilians.

Take Monday's Los Angeles Times story about how mistaken Predator video analysis helped lead to an inadvertent attack on civilians. It's a veritable play-by-play of how troops on the ground, drone operators, and other intelligence elements — all literally seeing and hearing different views of the same situation — misinterpreted and miscommunicated different pieces of data to misidentify a convoy of civilians as militants.

The biggest failure of the drone operators? Identifying the woman and four children under 6. It's incidents like this that are causing the controversies in Afghanistan and Pakistan over civilian deaths from drone strikes.

So if the problem is real, why is the Air Force offering only $20,000 to solve it? Probably because right now it's a problem that is so hard, the Air Force is just hoping for ideas.

Once it has a few that sound plausible it will take it to the Lockheeds and Northrops and Raytheons of the world to build out. Check back next year and there might be a $1 million challenge or a $10 million challenge — but that might be for a demonstration system a little more complicated than what you can build on your new Commodore 64.

Until then drone operators will continue to face hard choices every day about what they see and about what they should do — and hope that they are right.

"Better than basket-weaving..."
By Richard U. Wheeler
Monday, March 21, 2011 at 12:04PM

One of my best friends has a four-year old who is crazy about planes, and I can't wait until he graduates from middle school and I can say to him, "I want to say one word to you, just one word. Are you listening? Drones."

And then I can tell him about the rapidly growing number of drone educational programs. If you want to get into the drone business you can take courses in drone piloting, in drone maintenance, and even in drone design. And since drones are rapidly being adopted around the world, you might even be able to take your drone studies abroad—although that might be a problem when you graduate and try and get a security clearance to work for the US military, still the world's largest drone user.

But drones aren't just rapidly replacing humans in dangerous missions in the wars in Afghanistan and Iraq. They're also being used in environmental research missions that used to be performed by manned aircraft, everything from monitoring weather and the atmosphere and mapping forest fires, to mapping geologic fault lines and disaster areas. And more drones and more missions mean an increased demand for operators, maintainers, and designers.

Many new and developing drone missions can't be flown by military personnel and need civilian operators. So now academia—often in cooperation with the private sector and the military—has stepped in to fill the gap. You can find everything from minors that complement traditional aviation degrees to full-blown and fully accredited bachelors, masters, and now even PhD programs focused on drone use and technology. Here's the run down on some of your options—and some background on the links these programs have to defense contractors and the military:

Drone piloting

> University of North Dakota (Grand Forks, North Dakota), Department of Aviation
> BS in Unmanned Aircraft Systems Operations
> UND's program markets itself as the first bachelors in drone piloting. The program is essentially similar to UND's BS in Commercial Aviation with almost all of the electives filled by courses in unmanned aerial systems. Overall, UND has seven specialized drone courses. UND also runs an unmanned aerial vehicle training center at Grand Forks Air Force Base, which is partially funded with state monies.

Drone maintenance

> Northland Community and Technical College (Thief River Falls, Minnesota) Aviation Maintenance Technology Program
> Unmanned Aerial Systems Maintenance Technician Certificate
> Thief River Falls is only about 40 miles east of Grand Forks, site of UND's BS in Unmanned

Aircraft Systems Operations, and the two programs are featured together in background created by the Grand Forks Region Economic Development Corporation and the North Dakota Chamber of Commerce. NCTC (no direct relation to any other organization using that acronym) has six specialized drone maintenance courses, the most of any program.

Drone design

Oklahoma State University (Stillwater, Oklahoma), Department of Mechanical and Aerospace Engineering
MS and PhD in Mechanical and Aerospace Engineering Unmanned Aerial Systems (UAS)
OSU is one of the latest schools to offer a degree program, and is the first to offer a PhD. Both the MS and PhD programs are very similar to tradition MS and PhD programs in Aerospace Engineering, with the addition of two specialized drone courses. MAE runs the program in partnership with OSU's University Multispectral Laboratories (UML) a "a government-owned, contractor-operated (GOCO) nonprofit 501(c)3 corporation," which is funded in part by a five-year, $44 million contract with the US Navy.

Cranfield University (Bedfordshire, United Kingdom), School of Engineering
MSc by Research in UAS Platforms and Ground Control Station
Not many details are available about Cranfield's program, and since it is a MSc by Research there aren't specific drone courses per se. But one thing is clear—non UK/EU citizens need not apply, which isn't surprising considering the amount of defense research and study that goes on at Cranfield.

University of Southampton (Southampton, United Kingdom), School of Engineering Sciences
MSc Unmanned Vehicle Systems Design
Southhampton's MSc program is a taught program (as opposed to a research program like Cranfield's) which gives students opportunities to design both air and underwater unmanned vehicles. It is open to international students. And unlike many programs it advertises its industry affiliations quite openly, citing ties to British aerospace and sensor companies BAE Systems (makers of the MANTIS and the TARANIS), Rolls-Royce (maker of the engines for the Global Hawk), QintetiQ (maker of the high altitude long endurance (HALE) solar-powered Zephyr UAV, which can stay aloft for fourteen days at a time) and Cobham (which makes everything from sensors to new systems for autonomous air-to-air refueling).

General Drone Know-How

Embry Riddle Aeronautical University Daytona Beach Campus (Daytona Beach, Florida), College of Aviation
Minor in Unmanned Aircraft Systems
This program can be taken with an major at ERAU, which include many non-flying programs, but the minor alone will probably not get you certified to fly so you should probably go for a an aviation degree if you want to fly. Overall ERAU has five drone courses.

Indiana State University (Terra Haute, Indiana), Department of Aviation Technology

Minor in Unmanned Aerial Vehicles
Like ERAU, ISU's program is intended to complement an aviation degree, and the program prospectus notes that a private pilot certificate is "encouraged". The program has two drones courses.

Kansas State University, Salina Campus (Salina, Kansas), Department of Aviation
Unmanned Aircraft Systems program
K-State's program is the smallest of this group, with only three courses. But it also boasts an Aerosonde Mark 4.7 drone, the first unmanned aerial vehicle to cross the Atlantic Ocean—and links to the Kansas National Guard, the Kansas Air National Guard, and the Air Force Office of Scientific Research.

Drones Set to Invade National, State Parks
in WIRED's Danger Room
By Richard Wheeler
February 28, 2011 11:00 AM

When I was a kid going to summer camp in New York's Adirondack Mountains, I counted myself lucky if I saw a black bear once or twice in a season. But campers may soon be able to regularly see something bigger and badder when climbing the High Peaks: Reaper drones flown by the New York Air National Guard's 174th Fighter Wing based in Syracuse, New York.

And drones aren't just buzzing over the Adirondacks . The proposal to begin training missions there is part of a bigger push to build a drone infrastructure for flying missions throughout the United States. So new drone bases are being built. The FAA is setting aside airspace for drone flights. And you can even get an accredited college degree in roboplane repair or operations. (No word whether you can get advanced placement credit for using drones in Call of Duty, but check this space for updates.)

Today, most U.S. drones operate overseas in Iraq and Afghanistan, with rumors of drone use in Yemen, Somalia, and other regions around the Horn of Africa. Most of these are flown by the military — and a few by the CIA. But because of United States law and regulation, neither of these groups can easily fly drones within the United States.

National Guard units and civilian contractors could fly these missions, if only there was enough space and adequate facilities to train the operators and technicians required to do so. But that would require shifting resources and building new facilities. In other words, an opportunity for Congresscritters to bring home the cash for their states and home districts. The race for a piece of the growing drone pie has begun.

The latest example is the amendment proposed by Senators Charles Schumer (D-New York) and Ron Wyden (D-Oregon) to the "FAA Air Transportation Modernization and Safety Act" (S.223) that would increase the number of "National Airspace System" test sites from four to ten. At least one of these sites would have to include a "significant portion" of public land.

The Adirondacks, in Schumer's home state, clearly fit this bill. And not surprisingly, there is also a proposal to use the Juniper Military Area, located in Wyden's home state of Oregon, as another drone test area.

But Schumer and Wyden are, if anything, playing catch-up in a race that has already seen the establishment of unmanned aerial vehicle test and training sites at Grand Forks Air Force Base in Grand Forks, North Dakota; the National Air Intelligence Center in Springfield, Ohio; Langley AFB in Hampton, Virginia; Ellsworth AFB in Rapid City, South Dakota; Mountain Home AFB in Mountain Home, Idaho; and Whiteman AFB in Knob Noster, Missouri. Thanks to President Teddy Roosevelt and the establishment of the National Parks system, we can probably expect that the other 42 states not already mentioned will be competing to serve up some of their public land as drone proving grounds.

In addition to test and training sites, Federal education and stimulus money is being used to create nonmilitary drone education programs. The Department of Aviation at the University of North Dakota, located in Grand Forks and the operator of the test and training site at Grand Forks AFB, now offers the first Bachelors of Science program in Unmanned Aircraft Systems Operations. The Aviation Maintenance Technology program at Northland Community and Technical College, located in Thief River Falls, Minnesota just 40 miles east of Grand Forks, will soon offer courses in the repair of UAVs. Garrison Keillor will probably announce a new drone shop class at the high school in Lake Wobegon next.

Although it is hard to predict where the drone infrastructure will grow, if other defense contracting projects are a reliable guide, the drone-ification of America will probably continue until there is a drone aerodrome in every state and a drone degree program to go with it. Drone Scout jamborees and merit badges cannot be far behind — coming soon to a summer camp near you.

Photo: USAF

"The Effectiveness of CCTV Surveillance as an Anti-Terror Intelligence Tool: The 7/7 London Train Bombing Attacks, Today, and Tomorrow"

By Richard U. Wheeler
Thursday, November 1, 2007 at 03:00PM

Background

This paper was written in the fall of 2007 in Georgetown University's School of Foreign Service Security Studies Program. The assignment was to write a short analytical brief (no more than five pages) on a current topic in the area of technology and intelligence.

Abstract

The proliferation of CCTV surveillance technology has grown throughout the past decade, especially in the wake of Al Qaeda directed or inspired attacks in New York, Madrid and London. Proponents of this trend claim that these networks, combined with the new data mining and management software, create effective tools for both anti-terror and anti-crime operations. Detractors point to the failure of cameras to thwart major attacks in an anti-terror role as well as their limited value in an anti-crime role. This paper will assess the effectiveness of CCTV surveillance as an anti-terror intelligence tool in the 7/7 London Train Bombing attacks, and examine CCTV surveillance today and in the future.

The 7/7 London Train Bombings

On 7 July 2005 three bombs were detonated on the London Underground and a fourth was detonated on a London bus. The attacks killed 52 and injured over 700. "This is the worst terrorist attack in Britain," reported The Times, "The previous highest toll was in the 1974 Birmingham pub bombings, which killed 21."[1] A series of follow-on attacks planned by a different but related group was subsequently thwarted.[2] Although direct links to Al-Qaeda were not clear, both the successful 7/7 bombings and the failed follow-on attacks bore the hallmarks of Al Qaeda involvement that had been demonstrated on 9/11 in the United States and in the Madrid Train Bombings: massive simultaneous attacks against vulnerable civilian infrastructure.

CCTV surveillance prior to the bombings: anti-crime versus anti-terror approach

By 2005, the use of CCTV surveillance had reached a high level of coverage in the United Kingdom since its introduction in the late 1990s. However, even in the aftermath of the 9/11 attacks in the United States, the focus of most CCTV surveillance was as an anti-crime tool as opposed to anti-terror tool.[3] This is an important distinction for two reasons. First, although both criminals and terrorists commit criminal acts, their motivations can be different, which can cause different behavior patterns to produce similar results. Second, the response of the state to crime and terrorism varies and has changed over time.

For example, in the United States pre-9/11 state response to terrorism was framed in terms of law enforcement: terrorists were criminals in systems of states. They were often arrested, tried and convicted using the same systems the state employed against criminals. In this framework, anti-crime and anti-terror policies could and did share a number of common features. Post-9/11, however, the United States response has been framed in terms of war-making: terrorists are enemy combatants in a global, sometimes seemingly borderless battlespace. They are targeted for destruction and sometimes capture using the same systems the state employs against armed enemies (historically national armies). In this framework, anti-crime and anti-terror policies cannot and do not share as many common features.

A critical difference in the approach to information gathering in an anti-crime posture and an anti-terror posture is the end result of the intelligence it creates. In an anti-crime system, information is collected primarily to gather evidence to catch and prosecute criminals after a crime has been committed. Even though there are some moves afoot in the United Kingdom today to use CCTV surveillance in a more pro-active crime prevention role, cameras have generally been used in this fashion.

In an anti-terror system, by contrast, a major goal of intelligence collection is to prevent attacks before they happen. This means that the system must detect the indications and warnings of an attack, relay the information to active elements of the organization that are authorized and enabled to act, and then kill or capture or disrupt the terrorists before they strike. This distinction is especially important when looking at suicide bombings. If the attacker does not expect to survive, then he or she will most likely not be deterred by a system that is designed to capture and imprison him or her after their crime has been committed.

Effectiveness of CCTV surveillance as an anti-terror intelligence tool before the bombings

Clearly, CCTV surveillance was insufficient to prevent the 7/7 bombings. In this respect, its value as an anti-terror intelligence tool was low. Although 9/11 and the Madrid Bombings had clearly show that an attack like the 7/7 bombing's was possible, British officials were caught by surprise.[4] Certainly, CCTV may have had an impact on anti-terror operations that remains classified. But for the most part, its direct impact appears negligible, at least on the surface.

It can be argued that using CCTV surveillance in an anti-crime role still has indirect effects on countering terrorist operations, since terrorists sometimes also conduct criminal acts. However, the effectiveness of CCTV as an anti-crime tool has been questioned by numerous studies both in the United Kingdom and the United States.[5]

Effectiveness of CCTV surveillance as an anti-terror intelligence tool after the bombings

In-so-far as CCTV surveillance was able to help security forces conduct a forensic analysis of what happened, there was some value in that analysts could build a profile to use in screening for future attacks by other cells. Such work was essential in piecing together information that lead security forces to the second cell later in July 2005. In this regard, CCTV surveillance can play a role in anti-terror intelligence gathering. In general, after the 7/7 bombings, the volume of CCTV

surveillance in the United Kingdom has increased.[6] But based on its inherent limitations, it is unclear that an increased volume of coverage will result in an increased amount of actionable intelligence.

The future of CCTV surveillance

However, as seen in other technical intelligence collection disciplines (COMINT, IMINT, etc.) a greater volume of data does not necessarily lead to a greater amount of information, and a greater amount of information does not necessarily lead to a greater amount of intelligence. This is the classic "signal to noise" problem: how does the system of people and machines distinguish that which is important from the vast amount which is not.

This problem is even more acute when one attempts to use information collected from CCTV surveillance to create indications and warnings intelligence of events before they happen. A root problem of all technical collection systems is that as the number of sensors and the associated amount of data increases, the number of operators to analyze data does not necessarily keep pace.[7] And with sufficient numbers of operators (and the necessary training and infrastructure to support them), it is still difficult to create predictive intelligence. Even today, areas that are heavily monitored by human operators are still hit by terrorist attacks.[8] The essential problem is that a video image of a person walking down the street doesn't tell even a well-trained operator where a person is going or what they are going to do when they get there. In cases where the security forces do conduct aggressive profiling of potential terrorist targets, there are still a large number of "false positives" (or errors of commission) for every successful prediction.[9]

The dream of technologists is to increase the value of CCTV surveillance systems for both anti-crime and anti-terror intelligence operations by creating systems that can detect behavior.[10] This will entail the development of pattern recognition systems capable of scraping raw CCTV data feeds and creating information that can be fed to data mining systems and used as queries to databases. The complexity of performing these operations simultaneously on real-time data from literally thousands of feeds will be enormous. Despite the enthusiasm of the technical community, this day is a long way off. Although parts of the total system have developed in the past decade, we are still far off from the integrated system that can automatically tie enough information together to detect a terrorist in time to prevent an attack.

Conclusions

- CCTV surveillance did not significantly contribute to preventing the 7/7 London Train Bombings, although it did help prevent follow-on attacks.

- CCTV surveillance is better suited to anti-crime than anti-terror intelligence gathering (although its value as an anti-crime tool may also be low).

- The effectiveness of CCTV surveillance in either an anti-crime or an anti-terror role is decreased without adequate investment in infrastructure and human capital.

- There is a significant amount of technology development necessary to realize the dreams of creating CCTV surveillance based behaviors prediction tools.

[1] "Britain 'defiant' as bombers kill 52 in attack on the heart of London." The Times (London). 8 July 2005: Home News 2.

[2] Beaumont, Peter et al. "Police swoop on capital's estates as hunt intensifies: Two held as armed officers raid flats; Detectives seek link with African cell; 72 hours that shook London." The Observer. 24 July 2005. News, 2.

[3] Or simply as an anti-congestion tool: "There are more than 6,000 CCTV cameras monitoring every platform on the system, although Mr. McManus [head of policing and security for London's Underground] admitted that staff were more concerned with preventing dangerous overcrowding than spotting potential suicide bombers." (Tendler, Stewart, Webster, Ben and Evans, Michael. "Security officials ask: Could it happen in Britain?" The Time (London). 12 March 2004. Home news, 7.) An earlier article notes that "Mike Brown, London Underground's customer services director said that a spate of newspaper and television reports had blown the danger [of possible terrorist attacks on the Tube] out of all proportion" and that "…any measures taken to protect the network would need to be balanced against the need to move three million passengers each day as efficiently as possible." (Webster, Ben and Henery, Michelle. "Fear of terrorism attack on Tube 'is unwarranted'." The Times (London). 19 November 2002. Home news, 6.)

[4] "The Home Secretary, Charles Clarke, admitted that the London bombings had come 'out of the blue'. The security services, indeed, had recently lowered their estimate of the threat from 'severe general' " the third highest level " to 'substantial'. In the wake of the attack it was immediately lifted to 'severe general' again, but it was clear that there had been no warning." ("ATTACK ON LONDON: THREE DAYS AFTER THE SECURITY SERVICES 'LET IN A GOAL', THEY ARE STILL IN THE DARK." The Independent on Sunday (London). 10 July 2005. News, 6-7.)

[5] Gill, Martin and Spriggs, Angela. Assessing the impact of CCTV; Home Office Research Study 292. Home Office Research, Development and Statistics Directorate. 2005. Welsh, Brandon C. and Farrington, David P. "Surveillance for crime prevention in public space: results and policy choices in Britain and America." Criminology & Public Policy. Volume 3, 3, 2004. Both studies find that lighting may have as much or more effect on crime than CCTV surveillance.

[6] Today there are a reported 4.2 million security cameras in the United Kingdom today, or one camera for every 14 people in the country. It added "…recent studies found that every British citizen is caught by a camera's lens 300 times a day." ("Big Brother is Watching." British Heritage September 2007, Vol. 28 Issue 4: p.6.) Surveillance camera use is also increasing in the United States. The American Civil Liberty Union of Northern California notes that in California: "37 cities have some type of CCTV surveillance program. 18 cities have significant CCTV surveillance programs of public streets and plazas; an additional 10 jurisdictions are actively considering such expansive programs. 18 cities have systems in which the police actively monitor

the cameras." (Schlosberg, Mark and Ozer, Nicole A. Under the Watchful Eye; The Proliferation of CCTV surveillance Systems in California. American Civil Liberty Union of Northern California: August 2007: p.2.) The New York Civil Liberties Union reported that there were "nearly 4,200 surveillance cameras… below 14th Street [in Manhattan], more than five times the number counted in 1998." (Barron, James. "Civil Liberties Group Worries as City's Electronic Eyes Multiply." The New York Times. 14 December 2006: B03.) And in August 2006 47 cameras were being installed throughout Washington D.C., while about 80 cameras have been set up in Baltimore. (Cella, Matthew. "Spy cameras fail to focus on street crime." The Washington Times. 13 August 2006: A01.)

[7] For example: it is estimated that the average Briton is seem by camera 300 times a day. (British Heritage.) But how does that translate into tasks for operators? With a 2007 mid-year population of 61 million ("Data Finder." Population Reference Bureau. 27 September 2007. <http://www.prb.org/DataFind/datafinder7.htm>), 300 views a day creates over 1.8 billion views that humans need to process, or nearly 20,000 per second. With a combined police force of around 140,000 ("Police number reach record high." Criminal Justice System. 26 July 2005. 27 September 2007. <http://www.cjsonline.gov.uk/the_cjs/whats_new/news-3184.html>) this means that if every police employee in the United Kingdom stayed up 24 hours a day they would have to review one image every seven seconds (on more manageable eight hour shifts, this becomes a slightly more hectic two and a third seconds per image). Clearly, these numbers are inhuman, and police forces that use CCTV surveillance readily admit that they come nowhere close to reviewing everything the camera sees: "'We don't have time to sit and monitor these cameras at all times,' [Police Capt. Bob Keyes of the Clovis, California police department] said. 'There should be no expectation from the public that people are watching.'" (Bulwa, Demian. "Future fuzzy for government use of public surveillance cameras; still, some Bay Area cities hope to follow Clovis' lead." The San Francisco Chronicle. 23 July 2006.)

[8] "Last month, a Palestinian with bombs hidden under his clothing boarded a bus in Israel as a police surveillance helicopter hovered directly overhead. As the officers watched from above, he blew himself up and killed 19 people." (Goodheart, Andy. "Public cameras accost privacy." USA Today. 22 July 2002. 26 September 2007. <http://www.usatoday.com/news/opinion/2002-07-22-ncguest11_x.htm>)

[9] Fulton, Wayne. Personal Interview. 24 September 2007. Mr. Fulton, a private security consultant with extensive living and working experience in Israel and South Africa, spoke to me about undercover surveillance teams in Israel.

[10] "CCTV surveillance recordings from the Underground have been key in identifying the perpetrators. Yet given the possibilities of artificial intelligence, it's compelling to consider how a video camera infrastructure could be put to more advanced work in identifying and preventing terrorist threats." (David, Mark. "Electronics can protect subways against terrorism." Electronic Design. 04 August 2005: p.19.) Specifically, "The current shift from analogue to digital, computerized CCTV systems also supports expansion. Digital, algorithmic techniques, like those currently being used in the City of London's 'Ring of Steel' system and the system in Newham, East London, allow much larger systems to be automatically monitored because the systems can

be programmed to automatically search for ‘abnormal’ or ‘unexpected’ events, behaviors or even people. In the City of London, cars moving the ‘wrong’ way down a street automatically trigger cameras to monitor the scene. Additionally, by linking digit al CCTV with image database technology, ‘algorithmic’ CCTV systems can be programmed to automatically scan for specified faces or car number plates or to ensure that people are where they ‘belong’.” (Graham, Stephen. “CCTV: the stealthy emergence of a fifth utility.” Planning Theory & Practice. August 2002, Vol. 3 Issue 2.)