

NATURE & TECHNOLOGY**Unintended Consequences – Wexelblat Disasters**DIPLOMATIC PLANET INTERVIEW
WITH**Dr. Alan Wexelblat****Alan Wexelblat, Ph.D.****with David W. Alvey, Executive Director and Editor - Diplomatic Planet**

Introduction - Joel Garreau as a teacher, journalist, author and lecturer is well versed in looking at cultural revolutions and public policy. In his Washington Post article on September 2nd, 2001 "Nature's Revenge - Our Planet Has a Cure for Arrogance: It Makes Technology Into Our Enemy", Garreau looked at disaster from the perspective of "Nature's Revenge" and the "Law of Unintended Consequences".

Dr. Alan Wexelblat has been an observer-chronicler of the emerging pattern of disasters that result from Nature's vagaries and our own actions' "Unintended Consequences". Wexelblat's Law is wryly expressed as "When it comes to technological arrogance, nature has a nasty sense of humor". The resulting disasters - natural events that become magnified with effects that have unexpected large-scale impact on our man-made systems and our lives - can be attributed to the overload on Nature and the overexploitation or disintegration of a layer of relationships within its complex, inter-related network.

These twisted actions with dire consequences are called "Wexelblat Disasters" in (ahem) honor of the efforts of Alan Wexelblat who has popularized awareness of such events – as he, and we, look for signs of these long term, gradual shifts that build up consequences much as heavy flood waters can build up behind a dam. We see the water levels rise in the reservoir, but do we see the new channels being cut back upstream that will eventually circle around the dam, or the minute cracks in the dam walls that are straining and nearing collapse?

Our Disruptive Nature Finds the Weakness!

Integrating the human system into nature and the gradual build up of the consequences of our actions, per Garreau, fascinates Wexelblat - "Two trains banging into each other are dramatic. But the fact that the land is shifting and the rails are moving is harder to see". As further described by Garreau: "It's not the lightning that electrocutes you, it's the wire it knocks down. It's not the heavy soggy topsoil that gets you, it's the fireball from the ruptured underground gasoline tank.

It's not the floods that get you, or even the floods levitating the house off its foundation, it's the natural gas leak when the pipes break."

On September 12, 2001, the day after commercial airliners became adulterated tools of terror - I went back and re-read Garreau's article for its corollary on express human causes of techno disasters. Obviously, the actual domino-like calamitous consequences of the planes and their jet fuel bombs were not predictable events by these mass-murderers. A best ("worst") case scenario might have been for them to slice off a corner of a building, topple a wedge of the building, and to have a fire rage through the floors above. The results achieved - to take out the shell and the wall of structural supports coupled with the fierce intensity of the fire to cause both buildings to implode - becomes fantastic guesswork that could not possibly be directed or designed.

Dr. Wexelblat earned his doctorate at MIT's Media Lab where he designed and studied systems (sometimes called Community Support Systems or Digital Ecologies) to help people achieve working partnerships among themselves and with machines.

Per Dr. Wexelblat: "The basic notion is that you have a group of people, probably dispersed in space and time, who need assistance with an information-related task (search, browsing, navigation, retrieval, recommendation) and they turn over part of this task to computer systems that help them by finding, organizing, and recommending knowledge sources, including other people."

DPlanet: Dr. Wexelblat, am I reaching too far to relate "Nature's Revenge" and the "Law of Unintended Consequences" to the recent disaster at the World Trade Center in New York? Do those general issues of using common and benign technology to disrupt apply as we assess this entire scene?

Dr. Wexelblat:

I think there are two phenomena at work here.

One is best labeled as William Gibson put it in his mid-80s cyberpunk novels: the street finds its own uses for things. That is, given a device or system, the users of that device or system will adapt it to the purposes they have in mind, without regard for the intentions of the system designers/implementers/maintainers.

A good low-technology example: in Brazil, the phone company kept finding that the handsets were torn off its public phones. The reason turned out to be that someone had discovered that if you hooked up these handsets to a car battery and put it in the water it would emit tones that were very attractive to the kinds of fish that these fishermen wished to catch.

A more high-tech example of this is email. Supposedly designed just to carry messages it has now become a primary means of file transport (via attachments) of data storage (via people keeping large email inboxes or files of past email) and of spreading destruction (via the numerous Outlook viruses and worms of the past few years).

The second phenomenon is sometimes called the "Law of Unintended Consequences." This happens when large effort is exerted towards one effect, but a second effect happens - often opposite to what you desire.

Alan Wexelblat, Ph.D.

Dr. Wexelblat received a dual degree from the University of Pennsylvania: BSE Computer Science (School of Engineering and Applied Science) and BAS Philosophy and Science (College of Arts and Sciences). He received an MS from the MIT program in Media Arts and Sciences (Media Lab) Advanced Human Interface Group and his Ph.D. from the MIT Program in Media Arts and Sciences (Media lab), Software Agents Group.

His Doctoral Dissertation was titled "Footprints: Interaction History for Digital Objects" and "centered around the notion of using history information to help people solve present problems. I call this interaction history because it is the record of the interactions of people and objects."

Dr. Wexelblat has taught in graduate education programs at Boston University, Northeastern University and the University of Massachusetts; He has also been a commentator and contributor to several online discussions, and a technical editor/reviewer for O'Reilly, MIT Press, and SAMS Press.

Source: Dr. Wexelblat and Media Labs

It is my opinion that this "law" comes into play most often when people use technological systems, or legal systems, to try and enforce social change or policy (domestic or foreign). Two recent examples are these:

Recently, freelance writers sued over copyrights for their articles in online databases. In particular, the New York Times was a defendant, but the goal was to establish a US nation-wide legal precedent. The goal was to force these publications (such as the New York Times) to pay royalties for publication of the freelance articles.

The writers won, but the unintended consequence was that the New York Times refused to pay and simply stripped all freelancers' articles out of its online database.

Sadly, I fear that Osama bin Laden is an example of this same law. Our intention was to "contain" or "protect the world from" communism. In doing so we created, trained, and financed radical Islamic extremists who first turned to the production of heroin to finance their activities and, starting in about 1983 with the attacks on our troops in Lebanon, have now turned to massively bloody acts of terrorism against us.

The key difference I see is that the first kind of effect isn't really easily predictable. The second is, or should be. We need to focus not simply on achieving our goals but on doing so in ways that minimize the chances of unintended consequences arising.

DPlanet: Looking at evil intent and direct consequences - is there a logic to or a difference in strategy between attacking the hardware - denial of service attacks, disconnecting server clusters or telecom junctions - versus attacking the information and intellectual property itself - flooding sites with bogus info, wrapping propaganda in mainstream formats, or deleting en masse corporations and their workers?

Our limited experience in the types of losses that many of the companies resident in the World Trade Towers have experienced - where they have lost their institutional data files and the key personnel who represent the relationships and the institutional memory and practices - would suggest that most of these companies will fold within the next three years in addition to those that will not re open or will quickly go into

bankruptcy. Also, within the context of your interest in the effects of slow, less loud shifts in nature - Should we be more aware of this paradigm shift as we view our technology and its abilities to become destructive and disruptive of nature and its penchant to compound the natural consequences of weather, gravity, building cities near rivers and coastlines, clusterings of intellectual property, etc.?

Dr. Wexelblat:

I'm not sure these are comparable. It seems to me there are fundamental differences in kind, not merely in scale.

The fact of the matter is that the attacks on the World Trade Center towers were astonishingly low-technology. The weapons used - box cutters and small knives - could not have been stopped without banning all carry-on luggage and body-searching all passengers. Even then, ground crew servicing the airplanes could have been subverted to plant such weapons for later use.

What strikes me as sui generis in this case is that the "rules of the game" have changed. I simply don't see any successful hijack scenarios occurring in the future, because all air passengers now have been forced to realize that they may not get out safely and indeed their lives may be taken in the course of massive destruction.

The apparent downing of the UAL flight over PA as a possible consequence of passenger action shows us the likely course of future attempted hijackings of passenger craft. If we had wanted to prevent such a scenario the methods were well known before 9/11. El Al has an aggressive "air marshals" program coupled with reinforced airplane cockpits and training that the pilots must not leave the cabin while the passengers are on board. Boarding an El Al plane only happens after extensive luggage searches and intense questioning from motivated employees.

As a result it costs more to fly on El Al, but they don't get hijacked. In the US we turned airport and airplane security over to the airlines themselves. These corporations are legally bound to maximize their value to stockholders. Providing high levels of security was too expensive and it simply wasn't done. Security personnel at airports make something like \$5.75 per hour, less than some people working at McDonald's. Some low-price airlines pay their pilots only \$15,000-30,000 per year.

It is not hard to look at this and see how the law of unintended consequences has come to haunt us. Goal: cheap air travel; unintended consequence: severe vulnerability to terrorism.

If we wish to avoid this kind of thing happening in the future, we must look for such consequences. For example, if one consequence is a new willingness of airline passengers to fight hijackers to the death, then it is only logical to look for cases where a future hijacker could commandeer a similar plane without risking an aggressive hostile response from passengers.

To me this suggests cargo planes, such as the fleets operated by FedEx, UPS, and so on. If I was in charge of national transportation I would be insisting on massive increases in security on such planes, background checks on all employees, and much

tighter screening of cargo loaded into such planes. It doesn't take genius-level imagination to see that once in control of a cargo plane a terrorist could remove the benign cargo and load it up with explosives, such as the so-called fertilizer bomb used in Oklahoma City.

With that said, I do think there is a relationship between technology, technology analysis, and our response to these acts of aggression. Joel Garreau, who first interviewed me, has a very thoughtful piece in the Washington Post "Disconnect the Dots - Maybe We Can't Cut Off Terror's Head, but We Can Take Out Its Nodes" (2001-Sept-16) on using network analysis and network-disabling attacks against terrorist groups.

As to slow shifts in nature -- I think the sad context here is that we are forever fighting the last war, or countering the previous paradigm. Sailing aircraft carrier groups to Afghanistan is what I would call a "Maginot Line" response to these acts. We need to stop responding as if we were still fighting the last war and start responding as if we wanted to fight the next one.

Note that I do not say "win" because I think the old concepts of win and lose are not applicable here. We are in need of adapting some of the thinking that goes into designing systems in harmony with long-term shifts. We must design flexible responses, adaptive responses, and anticipatory responses. Having a US President standing up there saying we will "win" this "war" is as discouraging as it is absurd. Neither term applies to this situation.

The kind of thinking I think is needed to combat climate-change crises can also be applied to these kinds of situations.

DPlanet: You have expertise in looking at information management - searching for and accessing the needed information from the internet - and also in the security issues of privacy and shared access that also apply to the internet.

How will the fundamentals of access across the internet or the rules for personal privacy change as a result of these events - the unintended consequences?

Dr. Wexelblat:

I don't think the rules for personal privacy will change as a result of this event, except minorly at airports, where we've never had much in the way of privacy anyway. I've heard some pretty silly things in the last week, including airlines banning open beverage containers and requiring ID for infants. I confess I have a hard time seeing my 16-month-old taking control of a plane and I'm not at all sure how it helps anyone to hassle parents.

I also don't think the fundamentals of access online will change. The FBI will get more power to snoop into our lives. People will conveniently forget that the FBI and the CIA were not reigned in capriciously. They were reigned in because when unfettered they did more harm than good, both at home and abroad.

I continue to stress that this was a low-tech attack. CNN is now reporting that bin Laden has thrown away his cell phones, pagers, and other high-tech gadgets.

They're irrelevant to him. I don't understand why this point doesn't penetrate to people.

DPlanet: Do we have to work from a vulnerability mind-set?

Dr. Wexelblat:

Do you mean in the physical world or on the 'net? In both worlds we are vulnerable. While we discuss this, a new worm (currently being called W32.nimda) is busily wreaking havoc across the servers of corporate America. Like the airlines, these financially oriented entities have decided that real security is too complex and too costly. So they continue to be vulnerable.

DPlanet: How do we lock the cabin doors on the internet?

Dr. Wexelblat:

That's a cute metaphor but I don't think it's applicable. The Net far more resembles bin Laden's organization than it does an aircraft. The net is distributed, with some key nodes and massive redundancy. The story about it being designed to survive a nuclear attack is apocryphal, but nevertheless the Net has proven its resiliency against forms of attack ranging from distributed denial of service storms to misplaced backhoes.

DPlanet: Do we widen the digital divide by creating separate, multiple "virtual private networks" with very controlled entry and exits points and access levels?

Dr. Wexelblat:

This already exists. In the small, most corporations have VPNs already. Internet 2 is well underway, with strict access rules. The Web population has done a fabulous job of segregating itself already, with the top 100 or so sites absorbing a huge percentage of the traffic. None of this has anything to do with last week.

DPlanet: Does the communal internet have to die? Do we want financial transaction electrons roaring along the same optic routes as my email to you? Do we pull the plug on almost everyone so that same information route cannot be used from inside a terrorist's bunker?

Dr. Wexelblat:

No, yes, and no. In that order.

Terrorists don't inhabit bunkers, except on those rare days when someone is shelling them. They walk the same streets as you and I. They attend the same colleges, the same flight schools, sit in the same parks, and fly from the same airports. A mentality that says we can draw a line in the physical world and somehow put "them" on the other side from "us" is a fantasy.

Given that, there is no conceivable means by which the terrorists can be restricted from the 'net either. All we could do is cripple our most powerful recent engine of information freedom and economic progress.

DPlanet: Is it heresy to now say that we rely too much on technology?

Dr. Wexelblat:

Of course not. Many people have been saying this in many forms for a very long time.

DPlanet: I am sure that many people are looking at airport security procedures and saying - "Why didn't the computer pick up the fact that there were four middle eastern men paying for one-way tickets with cash at the gate - and trigger some warning?" Are we that technology sophisticated?

Dr. Wexelblat:

Again, there is a fallacious assumption here that somehow evildoers will kindly tattoo a mark on their foreheads or on their financial records that will allow us to identify them so we can draw that nice safe line separating us from them.

I'm sure these people all used credit cards, just like you and I. I bet they even had good credit histories, just like you and I. I'm sure they bought round-trip tickets, just like you and I.

This is the fallacy underlying so-called profiling, which used to be called "racial profiling" before someone realized that was a big stupid flag to march under. People are not statistics, and attempting to reduce the general to the personal leads to egregious errors and intrusions. Profiling has been a consistent failure every place it has been used.

DPlanet: Alternatively - Do we want "Big Brother" intrusions to take over human interaction and assessment? "Well, that's procedure!" -- By relying on a computer print out to challenge someone anonymously - what are we saying about the individual, culture and ethics?

Dr. Wexelblat:

Quite a bit, and much more than I have time and space to answer here. I will just point out that this is the normal state of affairs now. Again, I don't see massive changes coming about after the tragedy of 9-11.

DPlanet: What have we abdicated? What are the new points of conflict between inward looking self interest and outward looking self-expression? ... Personal Freedoms versus Group Security?

Dr. Wexelblat:

The conflict between the personal good and the group good has always been there. It's not a matter of chance that people consistently quote Ben Franklin on this. It just takes different forms at different places and times. What I think we've abdicated is the notion that anything other than the pursuit of money is noble, worthy of protection, or available as a priority. If you want to lay the blame for this at the feet of some god, lay it at Mammon's feet.

"I don't mind an environment where the ability to better oneself is available to all; what I find repugnant is that we consistently sacrifice all other goods, from personal safety to national preservation to that one goal."

If you want to see the new points of conflict, go watch an IMF meeting or G8 summit. The so-called leaders of the free world huddle in massive fortresses or behind ranks of shoulder-to-shoulder cossacks and the (corporate) press continues to report it as if nothing was amiss.

If you want to see the new points of conflict, go watch as a corporation (Adobe) uses the national police force (FBI) to arrest a foreign national (Sklyarov) for violating an absurd law (DCMA) when what he did wasn't even illegal in the jurisdiction in which he did it.

For all the death, destruction, and tragedy bin Laden and his followers are a drop of excrement on the buttock of the early 21st century. Aggrandizing them, or attributing to them consequences that were already well underway before he started running heroin, is just missing the point.

Bruce Sterling correctly pointed out that most ills of the present decade will be attributed to what he called "The Four Horsemen of the Modern Apocalypse: " ...drug kingpins, international terrorists, hackers, and child pornographers. bin Laden is just the most prominent example of one group.

DPlanet: Thank you. (DWA)

Originally published at www.DiplomaticPlanet.net
<http://www.DiplomaticPlanet.net/200805-0012.html>

This Document is available at
<http://www.DiplomaticPlanet.net/200805-0012.pdf>