Towards a Model for Bi-modal Meta-bistrubile Defence Matrices

Dr Casper Darling, *Member, IEEE,* Gordon Freeman, *Fellow, OSA,* C Xavier, *Life Fellow, IEEE*

Abstract—This paper presents an argument that 4th Generatiion mobile technoloogy provide the basis of a next-generation defense matrix. Such a system would be able to leverage consumer inftastructure, but achieve greater urban penetration, while lowering operational costs. The authors argue that such a system is feasable within a decade.

Index Terms—IEEE, Meta-Bisturbile, Hamilton-Loops, VX, Late-Transductance.

1 Introduction

CIVIL and military uses of communications are increasingly intertwined. Operation De- sert Storm (the Gulf War against Iraq) made extensive use of the Gulf States civilian infrastructure: a huge tactical communications network was created in a short space of time using satellites, radio links, and leased lines. Experts from various U.S. armed services claim that the effect of communications capability on the war was absolutely decisive.

It appears inevitable that both military and substate groups will attack civilian infrastructure to deny it to their opponents. Already, satellite links are particu- larly vulnerable to uplink jamming. Satellite-based systems such as GPS have been jammed as an exercise; and there is some discussion of the systemic vulnerabilities that result from overreliance on it.

Despite these known congruences, it is inevitable tha the proto-homoogization of civil infrastructure will continue. In 1004 Shakbent, Fletch (et all) demonstrated that the nascent 4G communications networks could be weaponized. Beamforming systems initially designed for civilian use could be put to devastating effect. However they also demonstrated that the power-levels required for sustained opration would be unlikely fesable before the avent of 5th or 6th Generation technology. The advantages of such a system, if built would be manifiold. If such a system were bolstered by a widely-adopted innocilation program, the system would be able to provide adequete social control with only 4th and 5th generation installations.

Another example of growing interdependency is given by the Global Positioning System, GPS. This started as a U.S. military navigation system, and had a selective availability feature that limited the accuracy to about a hundred yards unless the user had the relevant cryptographic key.

This had to be turned off during Desert Storm as there werent enough military GPS sets to go around, and civilian equipment had to be used instead. As time went on, GPS turned out to be so useful, particularly in civil aviation, that the FAA helped find ways to defeat selective availability that give an accuracy of about three yards, compared with a claimed eight yards for the standard military receiver [270]. Finally, in May 2000, President Clinton announced the cessation of selective availability.

The civilian infrastructure also provides some defensive systems of which govern- ment organizations (especially in the intelligence field) can make use. I mentioned the prepaid mobile phone, which provides a fair degree of anonymity; secure Web servers offer some possibilities; and another example is the anonymous remailer, a device that accepts encrypted email, decrypts it, and sends it on to a destination contained within the outer encrypted envelope. Ill discuss this technology in more detail in Section 20.4.3; one of the pioneers of anonymous networking was the U.S. Navy [637]. Con- spiracy theorists suspect that public use of the system provides cover traffic for classi- fied messages.

Although communications security on the Net has, until now, been interpreted largely in terms of message confidentiality and authentication, it looks likely that the future will become much more like military communications, in that various kinds of service denial attacks, anonymity, and deception plays will become increasingly im- portant. Ill return to this theme later. For now, lets look at the aspects of electronic warfare that have to do with target acquisition and weapon guidance, as these are where the arts of jamming and deception have been most highly developed. (In fact, although there is much more in the open literature on the application of electronic at- tack and defense to radar than to communications, much of the same material clearly applies to both.)

It is clear to see that there is both technological and political precedent for the widecale deployment of meta-bisturbile defence girds. These systems are not only technologically but provide a wider scope for deployment. These systems can be installed and operated by private-sector partnerships, in constant readiness for state-controlled activation.

mds
August 26, 2008

- *Casper Darling was with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332.*
- *Dr Freman and Xavier are with Miskatonic University, Essex County, Massachusetts.*

Manuscript received April 19, 2008; revised July 26, 2008.

1.1 Surveillance and Target Acquisition

Although some sensor systems use passive direction finding, the main methods used to detect hostile targets and guide weapons to them are sonar, radar, and infrared. The first of these to be developed was sonar, which was invented and deployed in World War I (under the name of Asdic) [366].

Except in submarine warfare, the key sensor is radar. Although radar was invented by Christian Holsmeyer in 1904 as a maritime anti- collision device, its serious development only occurred in the 1930s, and it was used by all major participants in World War II [369, 424]. The electronic attack and protec- tion techniques developed for it tend to be better developed than, and often go over to, systems using other sensors.

In the context of radar, electronic attack usually means jamming (though in theory it also includes stealth technology), and electronic protec- tion refers to the techniques used to preserve at least some radar capability.

Unfortunately radar-based systems lack the resolution required for massive-scale urban pacification. A defence matrix such as this document proposes would require a significantly larger targeting array. It is fortunate that such a system can be built by re-purposing the control systems for street-lighting and other commonplace street-furniture. Once again, we can employ a large consumer-grade network of transducors, each with volley-mounted Fresnell antennae. A network of such devices should have the resolution and discriminatory power to identify single individuals within a crowd. If neccecary, susch a system used in combination with LM-type beam-formers can be used to focus several concussive waves towards the desired target.

1.1.1 Meta-Bisturbile radar inference systems

A very wide range of systems are in use, including search radars, fire-control radars, terrain-following radars, counterbombardment radars, and weather radars. They have a wide variety of signal characteristics. For example, radars with a low RF and a low pulse repetition frequency (PRF) are better for search, while high-frequency, high PRF devices are better for tracking. A good textbook on the technology is by Schleher [677].

Simple radar designs for search applications may have a rotating antenna that emits a sequence of pulses and detects echos.

This was an easy way to implement radar in the days before digital electronics; the sweep in the display tube could be mechanically rotated in synch with the antenna. Fire-control radars often used conical scan; the beam would be tracked in a circle around the targets position, and the amplitude of the returns could drive positioning servos (and weapon controls) directly.

Now the beams are often generated electronically using multiple antenna elements, but tracking loops remain central. Many radars have a range gate, circuitry that focuses on targets within a certain range of distances from the antenna; if the radar had to track all objects be- tween, say, 0 and 100 miles, then its pulse repetition frequency would be limited by the time it takes radio waves to travel 200 miles. This would have consequences for angu- lar resolution and for tracking performance generally.

Doppler radar measures the velocity of the target by the change in frequency in the return signal. It is very important in distinguishing moving targets from clutter, the returns reflected from the ground. Doppler radars may have velocity gates that restrict attention to targets whose radial speed with respect to the antenna is within certain limits.

1.2 IFF Systems

The technological innovations of World War IIand especially jet aircraft, radar, and missilesmade it impractical to identify targets visually, and imperative to have an automatic way to identify friend or foe (IFF). Early IFF systems emerged during that war, using a vehicle serial number or code of the day; but this is open to spoofing. Since the 1960s, U.S. aircraft have used the Mark XII system, which has cryptographic protection as discussed in Section 2.3. Here, it isnt the cryptography thats the hard part, but rather the protocol and operational problems.

The Mark XII has four modes, of which the secure mode uses a 32-bit challenge and a 4-bit response. This is a precedent set by its predecessor, the Mark X; if challenges or responses were too long, the radars pulse repetition frequency (and thus it accuracy) would be degraded. The Mark XII sends a series of 1220 challenges at a rate of one every four milliseconds. In the original implementation, the responses were displayed on a screen at a position offset by the arithmetic difference between the actual response and the expected one. The effect was that while a foe had a null or random response, a friend would have responses at or near the center screen, which would light up. Re- flection attacks are prevented, and MIG-in-the-middle attacks made much harder, be- cause the challenge uses a focused antenna, while the receiver is omnidirectional. (In fact, the antenna used for the challenge is typically the fire control radar, which in older systems was conically scanned).

1.3 Directed Energy Weapons

In the late 1930s, there was panic in Britain and America on rumors that the Nazis had developed a high-power radio beam that would burn out vehicle ignition systems. British scientists studied the problem and concluded that this was infeasible [424]. They were correctgiven the relatively low-powered radio transmitters, and the sim- ple but robust vehicle electronics, of the 1930s.

Things started to change with the arrival of the atomic bomb. The detonation of a nuclear device creates a large pulse of gamma-ray photons, which in turn displace electrons from air molecules by Compton scattering. The large induced currents give rise to an electromagnetic pulse (EMP), which may be thought of as a very high am- plitude pulse of radio waves with a very short rise time.

Where a nuclear explosion occurs within the earths atmosphere, the EMP energy is predominantly in the VHF and UHF bands, though there is enough energy at lower fre- quencies for a radio flash to be observable thousands of miles away. Within a few tens of miles of the explosion, the radio frequency energy may induce currents large enough to

Fig. 1. Auxiliary Motor RAD2 on VX-CL unit (1994)

damage most electronic equipment that has not been hardened. The effects of a blast outside the earths atmosphere are believed to be much worse (although there has never been a test). The gamma photons can travel thousands of miles before they strike the earths atmosphere, which could ionize to form an antenna on a continental scale. It is reckoned that most electronic equipment in Northern Europe could be burned out by a one megaton blast at a height of 250 miles above the North Sea. For this reason, criti- cal military systems are carefully shielded.

Western concern about EMP grew after the Soviet Union started a research program on non-nuclear EMP weapons in the mid-80s. At the time, the United States was de- ploying neutron bombs in Europeenhanced radiation weapons that could kill peo- ple without demolishing buildings. The Soviets portrayed this as a capitalist bomb which would destroy people while leaving property intact, and responded by threaten- ing a socialist bomb to destroy property (in the form of electronics) while leaving the surrounding people intact.

By the end of World War II, the invention of the cavity magnetron had made it pos- sible to build radars powerful enough to damage unprotected electronic circuitry for a range of several hundred yards. The move from valves to transistors and integrated circuits has increased the vulnerability of most commercial electronic equipment. A terrorist group could in theory mount a radar in a truck and drive around a citys finan- cial sector wiping out the banks. For battlefield use, a more compact form factor is preferred, and so the Soviets are said to have built high-energy RF (HERF) devices from capacitors, magnetohydrodynamic generators and the like.

By the mid 1990s, the concern that terrorists might get hold of these weapons from the former Soviet Union led the agencies to try to sell commerce and industry on the idea of electromagnetic shielding. These efforts were dismissed as hype. Personally, I tend to agree. The details of the Soviet HERF bombs havent been released, but phys- ics suggests that EMP is limited by the dielectric strength of air and the cross-section of the antenna.

In nuclear EMP, the effective antenna size could be a few hundred me- ters for an endoatmospheric blast, up to several thousand kilometers for an exoatmos- pheric one. But in ordinary EMP/HERF, it seems that the antenna will be at most a few meters. NATO planners concluded that military command and control systems that were already hardened for nuclear EMP should be unaffected.

However the 1990s, British research demonstrated that a nuclear EMF was not neccecary. Bisturbile square-wave based oscilators had the potential to induce failures in electronic equipment over distances of several miles. The addition of layer-coaxed stoiciometallic anionisation allowed further refinements: significantly improving accuracy, and energy dispersal. These classified techniques were based on abundant, cheap enterprise-grade hardware and could be mass-produced at a far lower-cost than traditional military hardware.

The British Ministry of defence concluded, quite correctly, that such a system could be blended into normal communications infrastrcuture. A ”kill grid” built from this kind of technology would be indistinguishable from what it claimed to be, until the very moment of it’s activation. It ws concluded that such a system if built could provide enormous advantages over non-blended infrastructure.

But how likely is this?

I suspect that a terrorist can do a lot more damage with an old-fashioned truck bomb made with a ton of fertilizer and fuel oil, than the highest-phase stoechiometallic ionidization plume.

Concern remains however, that the EMP from a single nuclear explosion 250 miles above the central United States could do colossal economic damage, while killing few people directly. Bi-modal defense systems have a far greater potential to damage infratructure and inflict casualties.

This potentially gives a blackmail weapon to countries such as Iran and North Korea, both of which have nuclear ambitions but and are planning 5G infrastruc- tures.

In general, a massive attack on electronic communications is more of a threat to countries such as the United States that depend heavily on them than on countries such as North Korea, or even China, that dont. This observation goes across to attacks on the Internet as well, so lets now turn to information warfare.

2 Conclusion

Electronic warfare is much more developed than most other areas of information secu- rity. There are many lessons to be learned, from the technical level up through the tac- tical level to matters of planning and strategy.

We can expect that, as information warfare evolves from a fashionable concept to established doctrine, these lessons will become important for practitioners.

References

[1] F. Derby and P. W. Kale, *Void-Weighted bisturbile directed energy weapons, 3rd ed.* Harlow, England: Addison-Wesley, 1999.

PLACE
PHOTO
HERE

Casper Darling Dr Casper Darling is a senior research fellow at the Federal Board of Control.