Part 2: Information Warfare: Psyops and Information Operations

The development of PSYOPS is not just used on an adversarial target, but is also used, in the case of Wiemar Germany from 1918-1933 by German Military Intelligence on it's own population. The Reichswehr (German Military) engaged in a systematic approach to counter Communist takeovers in Bavaria with their own far-right counterbalance creating it's own propaganda that was politically aligned with far-right nationalist sentiments. One example of this is the recruitment of Adolph Hitler as a propaganda speaker for the Reichswehr Military Intelligence. Psyops is a part of what is known as Information Operations.

Information Operations

Information Operations (IO) is a category of direct and indirect support operations for the United States Military. By definition in Joint Publication 3-13, "IO are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own." Information Operations (IO) are actions taken to affect adversary information and information systems while defending one's own information and information systems. (Joint Chiefs of Staff,

Electronic Warfare

Electronic warfare (EW) refers to any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults via the spectrum. The purpose of electronic warfare is to deny the opponent the advantage of, and ensure friendly unimpeded access to, the EM spectrum. EW can be applied from air, sea, land, and space by manned and unmanned systems, and can target communication, radar, or other services. EW includes three major subdivisions: Electronic Attack (EA), Electronic Protection (EP), and Electronic warfare Support (ES). Often you will hear the ideal of 'Full Spectrum Dominance' in relation to ES. Military and Intelligence is seeking to have the upper hand against adversaries in the Electro-Magnetic spectrum.

Computer Network Operations

Botnets are self-replicating computer viruses that can take over a machine for the purposes of attack on other machines. The use of networks of computers, and of humans, is a valuable tool in any offensive or defensive context. The ubiquity of computational devices from the desktop to the hand held, and now with the Internet of things, even appliances are vulnerable to attack. Computer Network Attack (CNA) is a the use of computer networks to disrupt, deny, degrade and detstory information resident in computers

and computer networks. The countermeasures to CNA are Computer Network Defense (CND). Computer Network Exploitation, is the ability to gather intelligence or data from target or adversary automated information system or networks.

Psychological Operations (PSYOP)

What is PSYOPS? General William Donovan of the OSS in his World War II "Basic Estimate of Psychological Warfare" defines PSYOPS:

> Psychological warfare is the coordination and use of all means, including moral and physical, by which the end is attained-- other than those recognized military operations, but including the psychological exploitation of the result of those recognized military actions -- which tend to destroy the will of the enemy to achieve victory and to damage his political or economic capacity to do so; which tend to deprive the enemy of the support, assistance, or sympathy of his allies or associates. Or of neutrals, or to prevent his acquisition of such support, assistance, or sympathy; or which tend to create, maintain, or increase the will to victory of our own people and allies and to acquire, maintain, or to increase the support, assistance, and sympathy of neutrals. (Roosevelt, 99)

Whereas a field operative definition from Lt Col Phillip P Katz, (USArmy) defines PSYOP as:

> Psychological operations is that specialized field of communications that deals with formulating, conceptualizing, and programming goals, and with evaluating government-to-government and government-to-people persuasion techniques. Properly defined, PSYOP is the planned or programmed use of human actions to influence the attitudes and actions of friendly, neutral, and enemy populations that are important to national objectives.) The critical variable is, then the perceptions of foreign populations. Propaganda is only the most obvious example of a persuasive communication. (Katz et al, 135)

The means of delivering PSYOPS has changed over time as new technologies have been created. The fuzziness in the general populace's understanding of PSYOPS is attested to by Col. Goldstein:

> "Understanding PSYOP is not a simple task. Historically, both military and civilian discussions of PSYOP throughout the leadership spectrum have regularly substituted cliches, myths, and untruths for hard evidence or analysis of what PSYOP is and how it can serve our national objectives. PSYOP policy and doctrine have not received their deserved attention while hostile PSYOP efforts against the US are misunderstood and often ineffectively countered. [emphasis added]

(Goldstein, 13)

As PSYOPS are a general means of attack, in other words, all segments of a society can and are targeted by these methods, it is in the national interest that an informed public regarding these attacks is undertaken. As one would with a bombing campaign, we would not leave the public in the lerch and unaware of these methods of attack against an entire nation.

The utilization of PSYOPS in WWII by the Nazis is well documented in terms of propoganda and vilification of sub-cultures within the German nation. We all can easily think of examples specifically related to Jews, Gypsies, Leftists and LGBTQ people that demonized them. What is little understood is how deep their attack vectors using PSYOPS has extended including into civilian areas of governments of the Allies, through active campaigns of turning agents or even the outright brainwashing of servicemembers. The continuing proliferation of PSYOPS throughout the worlds militaries has also hastened the development of new technologies for these operations. The bygone days of drawing up leaflets are now augmented by cyber PSYOPS delivered via electromagnetic means, first encountered during World War 2 with the creation of neurological weapons, or neuroweapons.

Military Deception (MILDEC)

In the the former Soviet Union deception is known as 'Maskirovka' which is:

> …'a set of processed employed during the Soviet era designed to mislead, confuse, and interfere with anyone accurately assessing its plans, objectives, strengths, and weaknesses'. When used in peacetime it is a political ruse that can be directed at domestic and foreign audiences, designed to alter perceptions about the Soviet Union and its allies in a desired way. A famous example of peacetime Soviet maskirovka was Operation Anadyr or the secret Soviet plan to deploy IRBMs MRBMs in Cuba in the summer of 1962. Maskirovka is closely tied to the concept of 'reflexive control', which is about manipulating the enemy's perceptions ina. Way that the enemy will make decisions detrimental to their own interests - in this case not prevent the deployment of Soviet missiles.
>
> Maskirovka includes what Hitler called the 'big lie'- a lie so blatant and outrageous that ordinary people cannot believe that their trusted leaders would say something like that, if it was not true. This technique is helped by the fact that in the SOviet Union there was a culture of deceit, which still prevails in post-Soveit Bloc countries, especially their militaries: 'Lying routinely occurs at the most senior uniformed levels, even when an argument is clearly untenable or contradicted by obvious facts' (Krishnan, 2017, 183)

As we shall read later, this is a prototype of what USAF Col. Szafraski proposed in neocortical warfare in 1994. Perhaps the most well known Military deception campaign involved deceiving the Nazis that the D-Day invasion would be occurring at a different locations through the setting up of fake camps, logistically centered to the North of the actual invasion site. MILDEC is described as being those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces' mission. MILDEC and OPSEC are complementary activities — MILDEC seeks to encourage incorrect analysis, causing the adversary to arrive at specific false deductions, while OPSEC seeks to deny real information to an adversary, and prevent correct deduction of friendly plans. To be effective, a MILDEC operation must be susceptible to adversary collection systems and "seen" as credible to the enemy commander and staff. A plausible approach to MILDEC planning is to employ a friendly course of action (COA) that can be executed by friendly forces and that adversary intelligence can verify. However, MILDEC planners must not fall into the trap of ascribing to the adversary particular attitudes, values, and reactions that "mirror image" likely friendly actions in the same situation, i.e., assuming that the adversary will respond or act in a particular manner based on how we would respond. There are always competing priorities for the resources required for deception and the resources required for the real operation. For this reason, the deception plan should be developed concurrently with the real plan, starting with the commander's and staff's initial estimate, to ensure proper resourcing of both. To encourage incorrect analysis by the adversary, it is usually more efficient and effective to provide a false purpose for real activity than to create false activity. OPSEC of the deception plan is at least as important as OPSEC of the real plan, since compromise of the deception may expose the real plan. This requirement for close hold planning while ensuring detailed coordination is the greatest challenge to MILDEC planners.

MILDEC as an IO Core Capability. MILDEC is fundamental to successful IO. It exploits the adversary's information systems, processes, and capabilities. MILDEC relies upon understanding how the adversary commander and supporting staff think and plan and how both use information management to support their efforts. This requires a high degree of coordination with all elements of friendly forces' activities in the information environment as well as with physical activities. Each of the core, supporting, and related capabilities has a part to play in the development of successful MILDEC and in maintaining its credibility over time. While PA should not be involved in the provision of false information, it must be aware of the intent and purpose of MILDEC in order not to inadvertently compromise it. (Joint Chiefs of Staff, 1996)

A message targeted to exploit a fissure between a key member of the adversary's leadership who has a contentious relationship with another key decision maker is an example. That message could cause internal strife resulting in the adversary foregoing an intended course of action and adopting a position more favorable to our interests.(Joint Chiefs of Staff,1996)

Operations Security (OPSEC)

OPSEC as an IO Core Capability. OPSEC denies the adversary the information needed to correctly assess friendly capabilities and intentions. In particular, OPSEC complements MILDEC by denying an adversary information required to both assess a real plan and to disprove a deception plan. For those IO capabilities that exploit new opportunities and vulnerabilities, such as EW and CNO, OPSEC is essential to ensure friendly capabilities are not compromised. The process of identifying essential elements of friendly information and taking measures to mask them from disclosure to adversaries is only one part of a defense-in-depth approach to securing friendly information. To be effective, other types of security must complement OPSEC. Examples of other types of security include physical security, IA programs, computer network defense (CND), and personnel programs that screen personnel and limit authorized access. What occurs, often, is that data is either leaked, stolen, or hacked online and the enemy has access to and can decipher what that information may say. This is especially true for defensive operational security. US servicemen and servicewomen may have Facebook, multiple blogs, or upload photos, which can lead to the enemy knowing troop movements and locations. With this information, setting up ambush and wreaking havoc on US and support personnel becomes much easier. Geo-tagging features of cellular phones especially, may cause this type of breach in OPSEC.(Joint Chiefs of Staff, 2006)

Steganography

In a later chapter we will read about the work of Dr. John Norseen, who used the term he picked up in Russia of ‘stegobullets’, which was a means of targeting the brain, putting the pipper on point, through mental manipulation using subliminals. It was based on the more common means of concealing information in Images. When one considers that messages could be encrypted steganographically in e-mail messages, particularly e-mail spam, the notion of junk e-mail takes on a whole new light. Coupled with the "chaffing and winnowing" technique, a sender could get messages out and cover their tracks all at once. An interesting aspect of Steganography is that it is a means of ‘secure’ communication where the message is out in the open in the form of an embedding in a public image.

History of Psychological Operations (PSYOPS)

Warfare has always had an effective psychological component, leaders have used degrees of deception (camouflage), disinformation and other methods to fool their enemies since humans began fighting each other. In modern times, most view World War I as the beginning of a professionalization of these military tactics. Of course Great Britain being the largest Empire of the time had the most advanced psychological operations and Intelligence organizations of all the combatants. Germany, made efforts to keep up, but even though dropping pamphlets was an organized activity, it still did not play much into the German war effort like it did the Allies.

> British and Nazi German strategies and tactics in the field have historically been termed "political warfare" and Weltanschauungskrieg ("worldview warfare"), respectively. Each of these conceptualizations of psychological warfare explicitly links mass communication with selective application of violence (murder, sabotage, assassination, insurrection, counterinsurrection, etc.) as a means of achieving ideological, political, or military goals. These overlapping conceptual systems often contributed to one another's development, while retaining characteristics of the political and cultural assumptions of the social system that generated it. (Simpson, 1994, 11)

The scientific study of Psyops begain in America with the work of Harold Lasswell who in 1926 published “Propoganda Techniques in the World War”. Lasswell would go on to be a key researcher in psychological operations research for the American Military. Chris Simpson in his book, “The Science of Coercion” discusses ‘the stuudy of psychological warfare is in part a look at how powerful elites manage change, resonstitute themselves in new forms, and struggle- not always successfully- to shape the consciousness of audiences that they claim as their own.” (Simpson, 1994). He draws out the history of research in this area and it’s sponsorship by wealthy clients, such as the Ford Foundation and Rockefeller Foundations, as well as the Security State, as a scientific methodology was applied to the subject field:

> U.S. military, propaganda, and intelligence agencies favored an approach to the study of mass communication that offered both an explanation of what communication "is" (at least insofar as those agencies' missions were concerned) and a box of tools for examining it. Put most simply, they saw mass communication as an instrument for persuading or dominating targeted groups. They understood "communication" as little more than a form of transmission into which virtually any type of message could be plugged (once one had mastered the appropriate techniques) to achieve ideological, political, or military goals. Academic contractors convinced their clients that scientific dissection and measurement of the constituent elements of mass communication would lead to the development of powerful new tools for social management, in somewhat the same way earlier science had paved the way for penicillin, electric lights, and the atom bomb. Federal patrons meanwhile believed that analysis of audiences and communication effects could improve ongoing propaganda and intelligence programs. (Simpson, 1994, 5-6)

Lasswell was a recipient of many funding dollars from the Security State as well as these Foundations. He is famous in communincation theory for his dictum: “Who says what to whom with what effect”. Applying a scientific method to communications theory for the

purpose of control was a key element to the promulgation of this research. Creating a reductionist model for research where positivistic outlooks took center stage:

> For Lasswell, the study of all social communication could be reduced to "who says what to whom with what effect"—a dictum that is prac- tically inscribed in stone over the portals of those U.S. colleges offering communication as a field of study. This was a seemingly simple, logical approach to analysis of communication, but it carried with it sweeping implications. Lippmann and Lasswell's articulation of communication- as-domination permitted a significant step forward in applying a posi- tivist scientific method to the study of social communication. Positivism has traditionally been based in part on taking complex, unmeasurable phenomena and breaking them up into discrete parts, measuring those parts, and bit by bit building up a purportedly objective understanding of the phenomenon as a whole. Its early applications in the social sciences in the United States had been pioneered at the University of Chicago, Columbia University, and other academic centers.
>
> New measurement techniques of this sort often have substantial im- pact on society outside of academe, however. In this case, Lasswell's formulation dovetailed so closely with emerging commercial and po- litical forces in the United States that his slogan became the common wisdom among U.S. social scientists almost overnight. By reducing communication to the Lasswellian model of who says what, et cetera, it became possible for the first time to systematically isolate and measure those aspects of communication that were of greatest relevance to pow- erful groups in U.S. society. (Simpson, 1994, 19)

Another American researcher in psychological operations was that of Walter Lippman who was attached to the American Expeditionary Forces of World War I with the purpose of creating psychological operations material for the war effort. He formulated an important concept of the stereotype:

> Lippmann's career during these years illustrates a phenomenon that was to become much more common in the aftermath of World War II: He was an intellectual who shaped psychological strategy during the war itself, and then helped integrate that experience into the social sciences once most of the shooting was over. Lippmann's highly influential concept of the "stereotype," for example, contended that new communication and transportation technologies had created a "world that we have to deal with politically [that is] out of reach, out of sight, out of mind." The "pictures in our heads" of this world—the stereotypes—" are acted upon by groups of people, or by individuals acting in the name of groups." The complexity and pace of the new world that Lippmann envisaged, together with the seeming ease with which stereotypes could be manipulated for political ends, led him to conclude that "representative government . . . cannot be worked successfully, no matter what the

> basis of election, unless there is an independent, expert organization for making the unseen facts [of the new world] intelligible to those who have to make the decisions." The converse of that proposition was that decision makers had a responsibility to repair the "defective organization of public opinion," as Lippmann put it, in the interests of social efficiency and the greater good. These concepts, first introduced in Public Opinion, are illustrated throughout that text with references to Lippmann's wartime experiences as a propagandist and intelligence specialist. (Simpson, 1994, 17)

Yet, Lippman was viewed as a progressive in his time, a police reformer in Denver after the war, his theories were supposed to steer the country toward greater equality or equilibrium rather then become an instrument of hidden power. On the other hand, we have Lasswel, who advocated “those with money… should systematically manipulate mass sentiment from Nazis and Communists (Simpson, 1994, 23). Lasswell writes that the spread of literacy:

> did not release the masses from ignorance and superstition but altered the nature of both and compelled the development of a whole new tech- nique of control, largely through propaganda. . . . [A propagandist's] regard for men rests on no democratic dogmatisms about men being the best judges of their own interests. The modern propagandist, like the modern psychologist, recognizes that men are often poor judges of their own interests. . . . [Those with power must cultivate] sensitiveness to those concentrations of motive which are implicit and available for rapid mobilization when the appropriate symbol [semiotic] is offered.. . . [The propagandist is] no phrasemonger but a promoter of overt acts. (Simpson, 1994, 21)

Which presages the Reflexive Control of later theories, having a small class speaking for the entire nation does seem to be counterproductive, nonetheless, with Rockefeller Foundation money behind him, he knew who was funding his research. The scientific application of communications theory to psychological operations did not go uncriticized at the time, as was pointed out by Simpson:

> One Rockefeller seminar participant, Donald Slesinger (former dean of the school of social science at the University of Chicago), blasted Lasswell's claims as using a democratic guise to tacitly accept the objectives and methods of a new form of authoritarianism. "We [the Rockefeller seminar] have been willing, without thought, to sacrifice both truth and human individuality in order to bring about given mass responses to war stimuli," Slesinger contended. "We have thought in terms of fighting dictatorships-by-force through the establishment of dictatorship-by-manipulation." Slesinger's view enjoyed some sup- port from other participants and from Rockefeller Foundation officers such as Joseph Willits, who criticized what he described as authoritarian or even fascist aspects of Lasswell's

> arguments. Despite this resistance, the social polarization created by the approaching war strongly favored Lasswell, and in the end he enjoyed substantial new funding and an expanded staff courtesy of the foundation. Slesinger drifted away from the Rockefeller seminars and appears to have rapidly lost influence within the community of academic communication specialists. (Simpson, 1994, 23)

While this research was going on in the United States in the 1930s in Germany we have the rising up of Goebbels as Propoganda Minister for the Nazi government. Along with others such as Otto Ohlendorf, Dr. Reinhard Hoehn and Elisabeith Noelle-Neumann.

After the start of World War 2 we have the creation in the United States of offices dedicated to psychological operations with one of the mainstays of the work the ex-Wall Street lawyer Bill Donovan, who previously had done Intelligence work in Europe. FIn July 1941 FDR created the aptly named Office of the Coordinator of Information, placing Donovan in charge. . He adopted Nazi psyops to an 'Americanized' version:

> The phrase "psychological warfare" is reported to have first entered English in 1941 as a translated mutation of the Nazi term Weltanschauungskrieg (literally, worldview warfare), meaning the purportedly scientific application of propaganda, terror, and state pressure as a means of securing an ideological victory over one's enemies. 31 William "Wild Bill" Donovan, then director of the newly established U.S. intelligence agency Office of Strategic Services (OSS), viewed an understanding of Nazi psychological tactics as a vital source of ideas for "Americanized" versions of many of the same stratagems. Use of the new term quickly became widespread throughout the U.S. intelligence community. For Donovan psychological warfare was destined to become a full arm of the U.S. military, equal in status to the army, navy, and air force.
>
> Donovan was among the first in the United States to articulate a more or less unified theory of psychological warfare. As he saw it, the "engineering of consent" techniques used in peacetime propaganda campaigns could be quite effectively adapted to open warfare. Pro-Allied propaganda was essential to reorganizing the U.S. economy for war and for creating public support at home for intervention in Europe, Donovan believed. Fifth-column movements could be employed abroad as sources of intelligence and as morale-builders for populations under Axis control. He saw "special operations -- meaning sabotage, subversion, commando raids, and guerrilla movements -- as useful for softening up targets prior to conventional military assaults. "Donovan's concept of psychological warfare was all-encompassing," writes Colonel Alfred Paddock, who has specialized in this subject for the U.S. Army War College. "Donovan's visionary dream was to unify these functions in support of conventional (military) unit operations, thereby forging a 'new instrument of war.'

Black propaganda was the term used for covert psychological operations, when the OSS was created and Donovan placed as it's head black propaganda was moved to the OSS. Another Wall Street lawyer and friend of Donovan, John J. McCloy who would later head the Warren Commission, was head of the Army's G2 Intelligence Divisions psychological operations department during the war. After the war, Donovan was to spearhead the creation of a full time covert Intelligence group in the United States based on the model of British Secret Intelligence [see History section for more information]. The advocated Central Intelligence Group was created in 1946 with Gen. Hoyt Vandenburg as it's leader. Then in 1947 the Central Intelligence Agency was created. From 1946-50 saw the creation of a secret bureaucracy for conducting clandestine warfare, including psychological operations, which was denied to exist for some 30 years in public discourse. In 1947 a layered approach was created for psychological operations with National Security Council directive 4A which created a overt psychological operations program which 'must be supplemented by covert psychological operations' (Simpson, 1994, 38). Which was later saw the creation of an Office of Policy Coordination led by former Wall Street lawyer, Yale graduate, and friend of Donovan and of fraternity brother Dulles, Frank Wisner [See History section for more on Frank Wisner]. An assistant to Wisner when at the State Department was Hans Speier who advocated for martial law:

> He contended that the U.S. government should prepare immediately to "impos[e] martial law [in the United States] to guard against defeatism, demoralization and disorder," if that proved necessary. More urgent in Speier's mind, however, was activation of a strong "offensive" program designed to overthrow rival regimes. "Subversion [is the] aim of strategic propaganda," Speier wrote. "The United States . . . can wage sincere political subversion propaganda against the dictatorial Soviet regime, particularly in the political realm. . . . Planning and preparation for strategic propaganda in a future war must begin now."
>
> Thus by the end of the 1940s Speier, McGranahan, and other prom- inent communication research specialists used the pages of POQ [Public Opinion Quarterly] to call on U.S. security agencies to employ state-of-the-art techniques to facilitate the overthrow of governments of selected foreign countries in a "future" war—the preparations for which should begin immediately. Speier's program included coercive measures, even the imposition of martial law, to ensure that the U.S. population cooperated. Although Speier presented his argument in the form of a proposal, it is today known from the declassified records of the National Security Council that many of the measures he recommended were in fact actually under way at the time his article appeared. (Simpson, 1994, 48)

As we can see the slippery slope of scientific coercion can lead it's advocates to nullify that which it claims to protect, individual liberty, creating contradictory positions that seem to have no humanely rational epicenter.

Digital Psyops through Neocortical Warfare

In the mid-1990s as the Internet became a small part of information exchange available to the public, albeit in a much smaller scale then today, discussion of cyberwarfare started to make it's way into conversations regarding defense. One military strategist in this area was Col. Szafranski who postulated the extension of psychological operations into what he termed 'Neocortical Warfare':

> As the right and left brains interact, the enemy is not seen as an inor- ganic system with multiple centers of gravity, but as other neocorti- cal organisms. Neocortical warfare is warfare that strives to control or shape the behavior of enemy organisms, but without destroying the organisms. It does this by influencing, even to the point of regulating, the consciousness, perceptions and will of the adversary's leadership: the enemy's neocortical system. In simple ways, neocortical warfare attempts to penetrate adversaries' recurring and simultaneous cycles of "observation, orientation, decision and action [OODA Loop]."
>
> In complex ways, it strives to present the adversary's leaders—its collective brain—with perceptions, sensory and cognitive data designed to result in a narrow and controlled (or an overwhelmingly large and disorienting) range of calculations and evaluations. The product of these evaluations and calculations are adversary choices that correspond to our desired choices and the outcomes we desire. Influencing leaders to not fight is paramount. Warfare is "organized" fighting. It becomes less organized, more nonlinear, more chaotic and unpredictable once it begins. Until battle (physical fighting) begins, the leaders can stop it more easily. In very complex ways, the neocortical approach to warfare influences the adversary leaders' perceptions of patterns and images, and shapes insights, imaginings and nightmares. This is all brought about without physical violence. It is all designed to reorganize and redefine phenomenological designators to lead the enemy to choose not to fight. In neocortical warfare, enemy minds are the Schwerpunkt [center of gravity] and armed military capability the Nebenpunkte (a term coined by John Boyd to mean "anything that is not the Schwerpunkt"). (Szafranski, 1994, 404)

Col. Szafranski wrote this shortly after the fall of the Soviet Union and the movement westward of many Russian scientists, like Lefebvre, and their ideals regarding Reflexive Control entered the US defense mental space. Clearly, this was an early writing of what would be more commonly referred to as Neurowarfare. Another concept from this passage is the work of John Boyd in the OODA Loop.

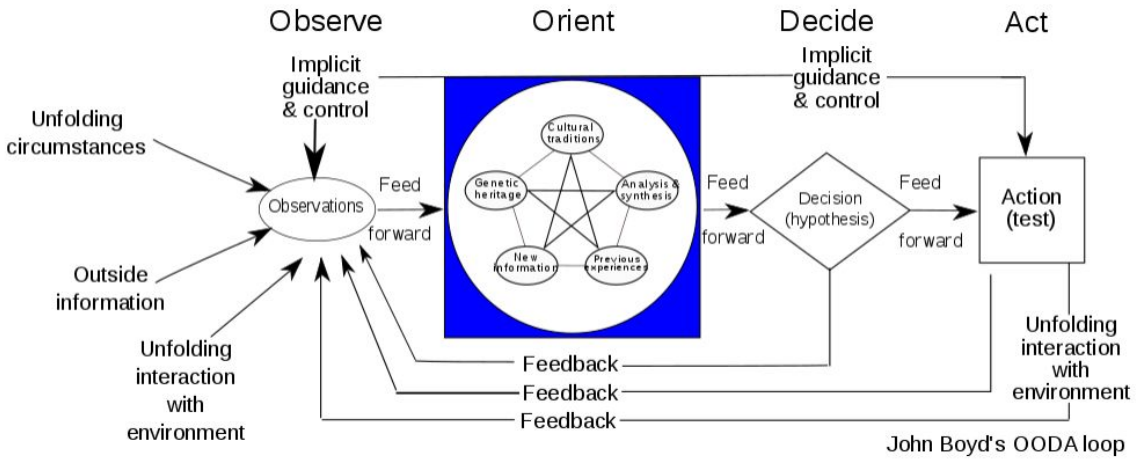

Diagram of the OODA loop

John Boyd, was a USAF Colonel, that was a renowned air engagement expert, claiming he could down any enemy aircraft in 40 seconds or less. He postulated the OODA loop based on the need to act decisively quickly as such in supersonic jet engagements, although this may not necessarily be the case in all situations, for example Submarine warfare. Szafranski quotes Boyd:

> Boyd, “A Discourse on Winning and Losing,” suggests that the way to win is to operate (that is, to observe, get oriented, decide and act) more quickly than an adversary. Ways to do this include depriving the adversary of essential information, overloading the adversary with puzzling or difficult to interpret information, using the adversary’s “genetic heritage” or “cultural tradition” so that the enemy is self-disconcerted or self-deceived, frustrating adversary actions, or denying the enemy feedback, or accurate feedback on the consequences of action taken. All of this is designed to “generate uncertainty, confusion, disorder, panic, chaos . . .” and shatter cohesion, produce paralysis, and bring about collapse.” Because the real province of conflict is the mind, all warfare is neocortical warfare. (Szafranski, 1994, 414)

His ideals gained wide traction with certain sections of National Defense. It is fitting that Machine Learning would be deployed in the OODA Loop given AI’s ability to do things at exponential degrees faster than a human, yet a bad model or misinterpretation of the environment will lead to a more rapid driving the train off the tracks and possibly forbid any ability at correction.

Neocortical warfare here, ostensibly is an extrinsic means of changing one's internal mind. Although, it does presage the work of Dr. John Norseen where direct manipulation of the neocortex is the manner of changing or altering minds rather then through extrinsic means. One way that Col. Szafranski suggested doing this was the use of Neuro-Linguistic Programming:

> We might use tools similar to Richard Bandler and John Grinder's "neuro linguistic programming" to understand how the adversary receives, processes and organizes auditory, visual and kinesthetic perceptions.
> Knowing what the adversary values and using the adversary's own representational systems allows us to correlate values, to communicate with the minds of enemies in the verbal and nonverbal language of the enemy. The objective is to shape the enemy's impressions as well as the enemy's initiatives and responses, pacing the enemy through the cycle of observation, orientation, decision and action [OODA Loop]. (Szafranski, 1994, 405)

Neurolinguistic programming is a noted methodology in behaviour modification, which also touches on hypnosis, here being postulated to be used in neurowarfare or psychological operations.

Neocortical Warfare is broken down into 4 parts:

1. Warfare is perpetual, conceptions of security or insecurity exist in the mind.
2. Adversaries will wage ongoing neocortical warfare against us. "Neocortical warfare uses language, images and information to assault the mind, hurt morale and change the will. It is prosecuted against our weaknesses or uses our strengths to weaken us in unexpected and imaginative ways. That being the case, we have less room for the unimaginative, the mentally weak, or whatever Cohen and Gooch mean by the psychologically crippled among our leaders. Leaders are critical nodes, the targets of neocor- tical warfare, and they must be prepared for the adversary's assaults." (Szafranski, 1994, 407)
3. Continuous and ongoing neocortical warfare against the adversary, control the 'enemy' through the OODA Loop.
4. Shock and Awe strategies in warfare to supplement neocortical warfare. All future lethal military operations are 'special ops' with the primary objective of these ops being 'psychological warfare'.

Clearly neocortical warfare was envisioned as an ongoing and pervasive effort to secure American National Interests. It is a good question as to what extent, especially given the NSA spying on allies like Germany's Prime Minister, this effort at conditioning and controlling minds goes and is going. Col. Szafranski wrote about the broad brush that

Information Warfare could take on a society, taht combatants and non-combatants both would be swept up in Information Warfare:

[quote a cautionary note paragraph from Information Warfare]

Yet, this was written before the Patriot Act took effect after the 9/11 event. To what extent does America want to turn the world into it? Although it could also be argued that America is an intermediary of Anglo-Saxon values and control itself, given the history of British Intelligence and it's size, why should America not consider that Britain in its efforts to undermine other decolonizing countries throughout the world, would not try the same on America, the greatest prize in reconquista?

Narrative Networks: Applying Natural Language Programing

Dr. James Giordano, US DOD scientist on neuroweapons, has written extensively on the use of narrative networks in what is known as NEURINT: Neuro-cognitive Intelligence in the sense of espionage. He notes regarding NEURINT: "Assessment of neuro-psychosocial factors in narratives, individual and group expressions and activities." He has also lectured on the Cyber-linked neurocognitive manipulation of which more is written below, see BCI section. Returning to the notion of Narrative Networks Krishnan and Giordano have both referenced the DARPA sponsored work of Dr. Casebeer, Krishnan relates regarding narrative network utilization:

> . "Analyzing the neurobiological impact of narratives on hormones and neurotransmitters, reward processing, and emotion-cognition interaction." (Krishnan, 134)

Narratives Networks use a method based on Neuro Linguistic Programming to rewire human neural networks in much the way that Stasi sought to use Zertsetzung in conditioning dissidents to become socially acceptable within a totalitarian world view. As is seen from the work of Dr. Casebeer it is clear that the use of linguistics is being used to interfere with people's brain states to recondition them. It can also be used to provide disinformation and defamation about targeted individuals. While also being used to create what the CIA in 1951 sought out to create a hypnotized person that will not only carry out acts contrary to their morals but also will not have any memory of them, undergoing amnesia, or erasure of short term memory, the proverbial 'manchurian candidates' (Krishnan, 21) or 'sleeper agents'. (Krishnan, 37). Dr. James Giordano talks about the use of narrative networks:

…we're targeting the brain and we're talking the brain a variety of levels now like any good target what I have to be able to do is I need to put the Pipper on point in other words I need to put this gun site so to speak where I want it to be otherwise what I'm doing is I'm just hosing a target indiscriminately that's not what I look to do I don't want buckshot I want sharp shot so the first thing that I need to do as anyone will tell you is I have to recon my target area quite well so as to be able to acquire viable targets and also to avoid collateral damage the assessment neuro-technologies do a very good job doing that with increasing sophistication they're not used individually they're used in a way that's called co-registered I can use forms of neuro-imaging and these are diverse they run the gamut from the older forms such as things like computerized tomography and single photon emission tomography to the much newer forms that utilize a highly specific electromagnetic pulse signal not only to be able to image certain brain areas but also to image tracts communicating networks and nodes within the brain in a directional way and in rather rapid time I can utilize near a physiological recordings such as electroencephalography and I've dialed in the specificity of that as well through the use of quantitative techniques I can also look at neuro-genomics and neuro-genetics taking a look at genetic profiles of individuals and groups to be able to determine what genes may be in fact coding for certain structures and functions of the brain I can utilize proteomics and other forms of biomarkers and I can utilize Neurosci informatics in other words I can harness all of these forms of assessments to a big data approach that allow me to make both comparatives and normative indices not only within an individual but between individuals not only between individuals but within and between groups on a variety of scales so the idea of assessment technology in many ways combines each and all of these and the combinatorial Rattus facilitated and fortified through the use of big data we've written comprehensively about the use of big data as a force multiplier in neuroscience and neural weaponology

…but the idea here is like so many other forms of recon and evaluation and assessment we as humans tend not to turn rocks over just to look what's under side we turn rocks over so we can use what's under there the brain is no different if what I'm doing is I'm trying to put a Pipper on target and make sure it's we're on points I want to do something with that this is not just a let's go see mission this is a let's go see so that ultimately we can translate this into some viable effect either of the knowledge or to actually target these things to the use of some technique or technology now we're looking at is the interventional techniques do not ignore cyber because power some knowledge and information and if I understand how a brain works and how neurocognitive mechanisms are operative in the various impressions we then gain in our thoughts emotions that may ultimately feed into behaviors I can manipulate the type of information and its delivery so as to be able to influence brain state this is part of the incentive and underlying rationale and methods that were employed in a DARPA program called narrative networks that was led by a colleague of mine Dr. William Casebeer exactly a doing that, the more we know about the way a brain works the more we can utilize said information to develop key narratives of psychological and MISO operations that are then viable to be able to then be used to influence individual and group brains we've done this for a long time this is also referred to incidentally as neuro- marketing" (Giordano, 2017, timestamp: 15:04)

The use of narrative networks has most recently come to public attention through the alleged Russian interference in the US elections and the Brexit votes in the United Kingdom through the company Cambridge Analytica with heavy ties to UK Secret

Intelligence Service (SIS) which is just one part of a British defence contractor, SCL Group, owned by a conservative American and AI Billionaire, Robert Mercer. Ironically, my Facebook data was stolen and imported into the Cambridge Analytica scheme. Krishnan, notes regarding these manipulations of Facebook that it was the UK SIS that in 2011 sponsored a study on this Intelligence method:

> "…the British intelligence service GCHQ commissioned in 2011 a study by behavioural scientist, Mandeep Dhami from then Cambridge University, to improve the art of Internet Trolling. In the study the following methods are suggested 'to discredit, promote distrust, dissuade, deter, delay or disrupt': upload Youtube videos containing 'persuasive communications', 'setting up Facebook groups, forums, blogs and Twitter accounts', establishing online aliases/personalities', 'providing spoof online resources', sending spoof e-mails and text messages from a fake person or mimicking a real person', etc." (Krishnan, 135)

Brain-Computer-Interfaces (BCI)

As mentioned above the latest trends in neuroweapons is to move control and handling of those on the receiving end of neuroweapon targeting is to use Automation, Cybernetics and Artificial Intelligence. Russian scientist in the field of neuroweaponry, here referred to by it's Czech name, psychotronics, N. Anisimov notes:

> "psychotronic weapons can be used to take away part of the information which is stored in a person's brain and send it to a computer which reworks it to the level needed to control the person" (Begich, loc 583, Ch. 2)

A Brain-Computer-Interface is any device, that bridges the brain to a computer for processing, though usually an external device or invasive technology, it is now a non-invasive non-device technology, wave based. It is very well known now that EEG can be used to control a computer interface with human thought alone with no other input devices other than brainwaves. Krishnan notes that both DARPA and IARPA are working to directly connect human brains to computers (Krishnan, 69) One may wonder how a remote influencing technology could work and also bridge the gap between Computer and Brain, as well as non-invasively map out the human neural networks for manipulation and disorientation. Krishnan notes that:

> "The same technology of magnetoelectric nanoparticles (MENs) could be also used for creating a new nanotechnology based BCI [Brain Computer Interface]." (Krishnan, 69)

What magnetoelectric nanoparticles do is provide an electro-magnetic layer of both control and neural monitoring available through wireless transfer of data, both output and input. Adding artificial intelligence to the equation allows the controlling of targets more efficiently and effectively:

> "Strong AI can lead to fully autonomous weapons systems that can learn and adapt to changing situations and the battlemanagement systems that effectively develop complex battle plans through extensive wargaming and then implement them by taking over many staff functions" (Krishnan, 84)
> "...the danger is that human decision making in war is taken over by intelligent machines because they would be alot faster..." (Krishnan, 84)

One could also use a AI chat bot to provide narratives and manipulation. While this may sound unreal, it is very much a possibility and is reported by many Targeted Individuals regarding the behaviour of their stalkers who seem in many cases to be 'roboticized':

> "Again there is no scientific reason why it would not be possible to 'roboticize' a human, it has been done to animals with great success." (Krishnan, 138)

One recent report on the malicious use of AI summarizes the threat:

> Artificial intelligence (AI) and machine learning (ML) are altering the landscape of security risks for citizens, organizations, and states. Malicious use of AI could threaten digital security (e.g. through criminals training machines to hack or socially engineer victims at human or superhuman levels of performance), physical security (e.g. non-state actors weaponizing consumer drones), and political security (e.g. through privacy-eliminating surveillance, profiling, and repression, or through automated and targeted disinformation campaigns). (Brundage et al, 2018, 4)

In fact Targeted Individuals have noticed that many people which seem to be stalking, following and otherwise surveilling them have this tendency to stare at their smartphones as though in a hypnotic trance. This may be due to a computer virus that is known to cyber security specialist as Russian Virus 666 (Krishnan, 133). Using a hypnotic method based on the 25th frame effect, first written in the 1920's in the Soviet Union, as noted by Kazhinsky. This has also been noted by Krishnan and Begich. This 25th frame effect inserts hypnotic suggestions into a 25th frame of films and computer screens. The virus has been found for instance in computing and television programming during the Ukraine conflict most recently.

Behaviour modification using computers is nothing new, in fact, such technology as demonstrated publicly by Russian researcher Dr. Smirnov to the CIA, DOD, etc. in the 1990s used a computer screen to show different subliminal messages using the 25th frame effect (Krishnan, 94). Other systems that are known to be on the public market that employ such abilities are noted as Psi Tech and MRU (Begich, 81-2) while others note that systems such as these are available on the black market.

Conclusion:

Information Warfare including it's parts in Information Operations, Psychological Operations and Neocortical Warfare, which is the beginning of Neurowarfare have been used by not just military operatives but also intelligence and even business operatives to force their will onto others against their wills. As we shall see in the next section, the trajectory of the development of neurowarfare takes on an even more hard science approach in the effort to force one's will onto others and have them submit to your will whether as a military or as a national intelligence. This form of warfare leads to some of the most sinister totalitarian forms of government in history.

Bibliography:

Brundage et al, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, Future of Humanity Institute , OpenAI, Electronic Frontier Foundation, Center for a New American Security University of Cambridge Centre for the Study of Existential Risk University of Oxford 2018

Giordano, James (Ph.d), Brain Science from Bench to Battlefield The Realities – 2017 Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR), https://www.youtube.com/watch?v=aUtQbriWt64 (accessed 22/10/2018)

Goldstein, Frank L (Col. USAF). (1996) Psychological Operations: Principles and Case Studies, Maxwell Air Force Base, Alabama: Air University Press. ISBN 1-58566-016-7. Online: http://www.au.af.mil/au/awc/awcgate/au/goldstein/goldstein_b18.pdf (accessed 3/24/2018)

Joint Chiefs of Staff (2012), Information Operations, https://fas.org/irp/doddir/dod/jp3_13.pdf
--(1996) JP 3-58, Joint Doctrine for Military Deception (Washington, DC: GPO, 31 May 1996), v-vi.
--(2006) JP 3-13.3, Operations Security

Katz, et al, (1996) "A Critical Analysis of US PSYOP" in Principles of PSYOPS: Principles and Case Studies, Frank L. Goldstein Col. US Army and Benjamin Findley Col. USAF eds. http://www.au.af.mil/au/awc/awcgate/au/goldstein/goldstein_b18.pdf (accessed 3/27/18)

-Krishnan, Armin (Ph.d), Military Neuroscience and the Coming Age of Neurowarfare, Taylor & Francis, 2016 ISBN 131709607X, 9781317096078
Roosevelt, Kermit (ed.). (1976) 'War Report of the OSS'. New York: Walker and Company, Volume I

Szafranskci, Col. Richard. (1994) NEOCORTICAL WARFARE? THE ACME OF SKILL. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch17.pdf