Variety Dynamics for Taking Control of Complex Heterogenous Systems in Information Warfare

T Love[1], T Cooper[2]

[1]*Design Out Crime and CPTED Centre, Australia*

Email: t.love@designoutcrime.org

[2]*School of Arts and Humanities*
Edith Cowan University, Australia

Email: t.cooper@ecu.edu.au

DOI: https://doi.org/10.5281/zenodo.17615160

Abstract: *This paper introduces the use of Variety Dynamics in information warfare. A central challenge of Information Warfare is to control situations using influence via information factors. Typical information warfare situations are a heterogenous mix of physical and informatic systems changing dynamically: with multiple owners/controllers of the different elements and whose power, skill, and allegiances change as do subsystems, elements, and relationships, including those with external entities. All of these are subject to change due to relationships within the situation and are also influenced from external locations, relationships, and motivations. These factors and structures are often opaque, hidden, or deceitful. Conventional systems or causal theories do not apply well to controlling such systems. Variety Dynamics is offered as an alternative method of influence, analysis, and control.*

Keywords: *Variety Dynamics, Two Feedback Loop Limitation, Locus of Control*

Introduction

Definitions of information warfare vary but centre on using information to confer military advantage (see, for example, Bingle 2023; Joint Chiefs of Staff 2022; Joint Forces Chiefs of Staff 2018; Congressional Research Services 2018; US Department of Defense 2022; US Marine Corps 2022; Wilson 2022). Information warfare is used in the short and longer term strategically and operationally (Betts 1982; Joint Chiefs of Staff 2022; Congressional Research Services 2018). The core practical strategies of information warfare are to manage information and information flows to normalise the desired interpretations of events. The information warfare approach contrasts with the bare use of force.

Information warfare supports conventional military approaches to taking control of situations by using force to gain ownership of the processes of control (Ames 1993; ICRC 2013; von Clausewitz 1984) as described for example in the UN Charter (Ekelhof & Paoli 2020). In such situations, information warfare is undertaken using SigInt (signals intelligence) and HumInt (human intelligence) along with misinformation and counterintelligence to provide advantage to those parts of the war-faring organisations delivering force to take or maintain control. Conversely, information warfare approaches can also be used defensively, for example, to support counter-intelligence, governance, and economic, social, and political processes (Alberts 1996).

The authors contend that accurate prediction of likely outcomes of information warfare

interventions is essential to effective conventional information warfare interventions and strategies. This is regardless of whether they are used defensively or offensively, and whether information warfare targets systems, interpretation of meanings (such as disinformation), or aims to produce behavioural changes or changes in the distribution of power.

There are three implications that follow from this.

- Prediction of consequences of decisions is required for planning information warfare interventions. Otherwise, information warfare interventions are in essence guesses whose outcomes (positive or negative) depend primarily on luck.
- Information gathering and analysis for information warfare done independently of prediction of consequences from decisions is likely to be ineffective or unnecessarily expensive, both financially and in terms of personnel.
- Ethical justification for information warfaring decisions depends upon reasonable efforts to accurately predict outcomes and consequences from strategies and interventions.

For the above reasons, this article focuses initially on this role of prediction of outcomes in information warfare and the limitations that emerge for complex and hypercomplex information warfare situations. Later, it outlines how Variety Dynamics can contribute both to improvement of prediction in information warfare and, more importantly, to achieving the intended aims of information warfare.

Some Limitations to Effective Information Warfare Decision Making

Information warfare operates in a complex context in which reality is contested. In fact, managing this contest of reality is the central role of information warfare, especially in the realm of counterintelligence (Alberts 1996; Bingle 2023; Brooker 2021; Joint Forces Chiefs of Staff 2018; Congressional Research Services 2018; US Marine Corps 2022; Wilson 2022).

In spite of the obvious potential benefits of information warfare methods, Krishnadas (2021) has noted that information warfare approaches have had a history of failure in situations of increased complexity such as counterintelligence, which can be considered as adding to complexity.

Information warfare decisions about interventions are grounded on justifications based on prediction of outcomes and consequences resulting. Decisions are typically made by those with the necessary authority based on their mental prediction of consequences.

When information warfare situations become complex, systems theories and Systems Thinking methods are increasingly used to support information warfare decision making (Brooker 2021; Engstrom 2018). The systems research literature, however, has expressed ongoing concern of cognitive limitations to mentally predicting outcomes of complex situations and undertaking valid and effective decision making in complex contexts (Cronin, Gonzalez & Sterman. 2009; Doyle *et al.* n.d.; Papachristos 2019; Shipman 1981; Sterman 2006, 2018, 2002).

Over fifty years ago, Forrester (1972) identified that decision makers in complex situations most commonly made decisions opposite to those that would produce the intended results. More recently, Cronin and colleagues (2009) identified that even individuals with substantial cognitive abilities and skills have difficulty predicting outcomes and making correct decisions, even at the lowest levels of situational complexity (situations with a single feedback loop).

Love (2010a, 2010b, 2018, 2023a) has identified a limit to human cognitive ability to mentally

predict outcomes where situations have two or more feedback loops. That is, humans can commonly predict behaviours and outcomes for information warfare situations whose behaviour is shaped by a single feedback loop or no feedback loops. It appears that, biologically, this is the limit to human cognitive ability and humans are unable to predict the behaviour and outcomes for information warfare situations shaped by two or more feedback loops. Love has coined this as the Two Feedback Loop Limitation axiom (Love 2009, 2010).

This Two Feedback Loop Limitation is axiomatic because it is self-evident from phenomenological observation and confirmed by comparing calculated consequences of one and two feedback loop situations with human participants' mental predictions of the consequences (see, for example, Cronin, Gonzalez & Sterman 2009; Sterman & Sweeney 2007). This identification of a biological limit to prediction associated with feedback loops follows Forrester's (1972) earlier observations and those of Sterman and colleagues (Sterman 1989, 1991, 2002; Sweeney & Sterman 2000). It is also supported by the extensive research in the U.S. and in Europe on cognitive limits to decision making in complex situations (see, for example, Buschman *et al.* 2011 ; Cronin, Gonzalez & Sterman 2009; Keane & Thorp 2016; Pursiainen & Forsberg 2021; Schmid *et al.* 2011; Simon 1957; Sterman & Sweeney 2007).

Also obvious from observation is that there appears to exist a widespread self-delusion in regard to this cognitive limitation. Regardless of their failure to predict outcomes in multifeedback loop situations, people report that they have correctly predicted outcomes, and that in general such prediction could be achieved if only sufficient mental effort was applied. This self-delusion aligns with the broader erroneous belief that human cognition and creativity is unlimited.

A corollary of the Two Feedback Loop Limitation above is that teams are no better than individuals at predicting consequences from decisions for interventions in complex situations. Every member of the team is subject to the same cognitive limitation in regard to his or her predictions.

Taking a different viewpoint suggests that the primary role of group discursive decision making for complex situations may not be prediction and achieving success in decision making; rather, it may be seen as a process to agree to share blame for the faulty predictions (see, for example, Shannon, McGee & Jones 2019).

A second limitation to effective information warfare decision making occurs when the structure of an information warfare situation does not conform to the assumptions required for the application of systems thinking methods. The authors refer to such situations as 'hyper-complex'. Conventionally, prediction, analysis, and decision making about intervention in situations are underpinned rare and is non-existent in hyper-complex situations. As the number of elements, relationships, and other changes in the situation increases, the mathematical difficulties and time taken to predict outcomes from decisions increases exponentially. To some extent, this latter limitation is increasingly addressed by increases in computing power, improved mathematical predictive power, the use of Artificial Intelligence methods based on very large data sets, automation of large-scale analyses and predictions, and improved user interfaces with these automated systems such that their use does not require high levels of technicality. This latter can be seen in the AI-assisted algorithmic targeting system, Lavender, currently used by Israel in the conflict in Gaza. The limitations of using such AI methods, however, are the same as described more fully earlier.

Hyper-Complex Information Warfare Situations

Hyper-complex situations are subject to a variety of power and control influences involving a

dynamic, continuously changing arrangement of constituencies, power holders, actions, decisions, stakeholders, system structures, sub-systems, elements, relationships, purposes, roles, and ownerships with amorphous boundaries in which all the above may be influenced by and influence elements beyond those boundaries. Hyper-complex information warfare situations are those whose structural and functional characteristics lay outside the conventional systems' assumptions necessary for the use of causally based methods of systems analysis and predictions of consequences used by systems thinking methods. Typically, this means one or more of the following are characteristic of the situation:

- Changing and porous system and subsystem boundaries.
- Subsystems and system elements come and go, overlap, change purpose, ownerships, relationships, and dependencies.
- System purposes, ownership, and role changes over time.
- Multiple feedback loops that change.
- Behaviour is sensitive to initial conditions.
- Sometimes the subsystems elements and system do not operate in ways that can be explained causally.

In general, hyper-complex situations have non-linear, multiple, dynamically changing, feedback loops between subsystems, system elements, processes, the system itself and factors that lay outside the system boundary. This means hyper-complex situations are usually outside the realm whose behaviours can be understood and predicted.

Many information warfare situations can be considered hyper-complex because they align with the above: their structures and context are not static; multiple feedback loops are common; characteristically they do not conform to the assumptions necessary for Systems Thinking analysis; and they are typically sensitive to small changes in conditions. Often they consist of a number of interested constituencies with complex and changing relationships between them that are situated within larger organisational arrangements (such as agencies, States, or nations) with a variety of complex political, geopolitical, commercial, diplomatic, power relations, power holding groups, informatic relations, and power projecting forces—all applying and subjected to differing and dynamically changing power and control arrangement that are also responding to changes elsewhere.

In considering the complexity and hyper complexity of information warfare situations, think for example of Afghanistan and its relationships to Iran, the U.S., Pakistan, India, and the sundry religious, political, warlord, and tribally based factors, its different cultural pressures, geopolitical transitional imperatives together with election issues in major players such as the U.S. and UK, for example. Similarly, think of the historical issues in Vietnam, or the tensions in the problems for Australia in relation to Indonesia, Malaysia, Timor-Leste, China, and Russia and the fossil fuel and chemical companies and political elites with interests. Or diplomatic tensions in the Middle East with its changing patterns of relationships in which now Iran and Saudi Arabia are closer partners or more distant enemies. Or the international shifts in power across the world, especially in Europe, Africa, India, and South America, resulting from the mixed dynamic financial, informatic, and kinetic war interventions following Russia’s invasion of Ukraine and Israel’s intervention in Gaza, West Bank, and Lebanon following Hamas’ attack in Israel. In each of these cases, the complexity and hyper complexity of information warfare is driven also by the complexity and hyper complexity of the situations. Another example is the variety of different roles and interests

of the U.S. and its commercial interests in South America—along with Iran, China, and Cuba, for example. Or think solely of the political and economic relationships in Africa, particularly West Africa, with the ongoing commercial and security interventions by the U.S., France, and Russia. Hyper-complex situations are, in many ways, the most common decision-making contexts in information warfare.

It might be argued that, given enough data (big data), or by using ensemble modelling via, for example, agent-based modelling, neural net modelling, or machine learning AI algorithms, it should be possible to identify likely potentially successful information warfare decisions. However, there are several limitations on the validity of such AI guidance in hyper-complex information warfare situations.

There are potentially several Artificial Intelligence (AI) methods that might be applied to predict the outcomes of information warfare decisions and to guide such decision making. All of these, however, require substantial amounts of accurate and reliable data to train the AI system or to identify patterns.

The need for accurate unbiased historical data as the basis for AI decision support can be seen in grammar and spell checkers and automated text generation software, which all, behind the scenes, use very large amounts of well-cleaned data to inform their algorithms. In each, they depend for their activities on using millions of samples of cleaned data to predict what word, letter, or sentence should occur next. Typically, prediction is done using variants of Bayesian analysis to identify the combinations of letters or words most likely to satisfy the required outputs. Similar processes are used by general transformer processes (such as ChatGPT), machine learning, and big data analyses.

The accuracy of AI predictions depends crucially on accurate, reliable historical data that is an unbiased valid representation of the real-world situations. Problems that occur when historic data is flawed can be seen in the failures of facial recognition in and the failure predictive policing algorithms. Police facial recognition systems have been mainly trained on white male faces, and this resulted in high levels of false positive identification of non-white faces and females and different demographics (Grother, Ngan & Hanaoka 2019). Predictive policing algorithms have problems resulting from a similar problem of biased data (Hung & Yen 2023). For example, in the U.S., the AI software was trained on historic data that included substantial over-policing of non-white residential areas. The use of biased data resulted in bias in the predictive policing algorithms such that it increased the over-policing problem in a similar way to how social media algorithms result in increasingly extreme content being provided to users.

The use of AI in hyper-complex situations, such as information warfare, can be especially sensitive to erroneous and unrepresentative historical data. This is because in hyper-complex situations there are in addition ongoing dynamic changes in the situation's architecture and structure, the elements in the situation and their relationships, ownerships, and purposes. These changes are additional sources of change in addition to the normal changes in variables. As a result, hyper-complex systems have much greater sources of variability, resulting in increased sensitivity to small changes, including starting conditions and, as a result, predictions can easily and frequently be extremely erroneous (see, for example, Palmer 2022). In information warfare, this results in more extremely faulty predictions and advice and decisions that are potentially problematic and dangerous. The above does not, however, include saturation mass misinformation and disinformation strategies, for example, as implemented through print, digital, audio, or social media whose intention is more like mass propaganda and, in essence, is functionally of one or less

feedback loops.

There are also background problems with the use of AI methods as the basis for decision making in information warfare. For example, in most AI methods there is no access to the explanation of the underlying reasoning for the specific prediction or advice from the AI system. In mentally reflecting on decisions made using conventional thinking, it is possible to backtrack to find errors or to use such reflection to better understand the situation in focus and to learn to make better decisions. AI systems, however, typically comprise opaque 'black or grey box' processes that are not decomposable back into explanations of the underlying reasoning. In this case, it is not possible to use the AI systems to mentally 'understand' why something worked or didn't work and this means AI systems do not provide learning and evolutionary advantage in the prediction of outcomes necessary for making valid strategy or intervention decisions.

A corollary of the above is that the dynamic nature of hyper-complex systems means it is not easily possible to identify whether the outputs of the AI methods are valid or correct, which is an additional challenge to the use of such systems.

Variety Dynamics and Information Warfare

In the past, information warfare decision makers and strategists have addressed the reality of hyper-complex situations by simplifying them to align with conventional systems' assumptions to enable them to be thought about more easily. The fact that this simplification can result in deeply flawed understanding, prediction, and decision making is easily overlooked and can, in some cases, lead to disastrous results. An example is the simplification that led to disastrous results for Hezbollah in 2024.

Example of Failure Due to Simplification in Information Warfare: Exploding Pagers and Radios in Lebanon 2024

The management of Hezbollah became concerned that Israel had the ability to conduct information warfare by access to the mobile phone communications of Hezbollah staff via Pegasus or similar software. As protection, they decided to revert communication to pagers and handheld radios as an information warfare defence. Following a conventional system thinking approach to information warfare, Hezbollah considered the provenance of the supply chains for the purchase of the devices, checked the purchasing process, and physically reviewed the devices. These are all the necessary typical steps in managing potential options for risk— presuming the situation behaved according to conventional systems thinking assumptions.

In fact, however, Israel, had increased the variety of options in this information warfare situation with Hezbollah by ahead of time arranging a parallel supply chain for devices to be constructed with remotely triggered explosives that were hard to detect. Alongside that, Israel created credible but false advertising and purchasing arrangements arranged to ensure the weaponized pagers and radios were the preferred purchase for Hezbollah staff members. The forcing of the considerations of information warfare into a conventional systems analysis approach was disastrous for many Hezbollah members and for innocent people who stood nearby. Had Hezbollah taken the view that they situation was potentially hyper-complex, it may have addressed it differently and reduced the risks.

To date, oversimplification of situations to fit the assumptions of systems thinking has been primarily because there has been no well-developed alternative for managing hyper-complex information warfare situations. This lack has resulted in poorly fitting approaches, such as the above, leading to faulty prediction of the likely consequences of information warfare decisions and

interventions.

The problem of over-simplification of the factors in a situation to facilitate analysis is similarly found in the use in information warfare of mathematically based modelling from fields such as those of Operations Research. Such mathematical modelling also typically simplifies hyper-complex situations to address the limitations of the modelling and computation.

To recap, a primary purpose of information warfare is to influence the locus and ownership of control and power as a substitute for, or in collaboration with, the use of force. Variety Dynamics was developed over the last 20 years by Love (2023b, 2007a, 2007b, 2008) and Love and Cooper (2011a, 2011b, 2021, 2023a, 2023b, 2024) as a practical approach to support decision makers to change the locus and ownership of control and power whilst also going beyond the limitations of conventional information warfare approaches outlined in the previous sections. Variety Dynamics was developed to be effective in both conventional and asymmetric power situations in ways that result in an additional, potentially more effective dimension to information warfare.

The primary focus of Variety Dynamics in information warfare is the distribution and dynamics and ownership of *variety* in information warfare situations and surrounding contexts. The *variety* in Variety Dynamics refers to options available to any element of a situation at any specific time. For example, if information could be held in either a Word, PDF, or JPG file, then the number of options of file type, (in other words, the *variety* of file type is three). Similarly, if data could be held on a laptop, desktop, in-house server, or cloud server, then the *variety* of the choice of options for storage of data is four.

The central understanding of Variety Dynamics is that the distribution, dynamics, and ownership of variety in a situation shapes the location, trajectory, and ownership of power and control. This can be seen most obviously in the simplest case where, to have control, a manager must have more variety than the variety generated by those being managed. Otherwise, those being managed can do things for which the manager has no response. In the latter case, the locus and ownership of power flows away from the manager and towards those being managed.

By focusing on *variety* rather than causal relations, Variety Dynamics offers a very different basis for prediction, decision, and strategy making. By observing the distribution, dynamics and ownership of variety in a situation, Variety Dynamics can be used to understand the location, trajectory, and ownership of power and control during the normal operation of a situation, regardless of its complexity or causal relations. This understanding of the distribution, dynamics, and ownership of variety (the options available to different constituencies at different times) provides the basis for deliberately changing variety distribution in ways that in turn result in changes to the location, trajectory, and effective ownership of power and control.

Variety Dynamics offers new and potentially more effective strategies for conducting active and defensive information warfare, SigInt, HumInt, and cybersecurity intelligence than traditional causal approaches. In parallel, Variety Dynamics also offers an additional basis for the description and management of all forms of signals and human intelligence: analogue and digital. Variety Dynamics applies to information warfare decision making and general warfare strategy making, including diplomacy, deal making, power management and the shaping of influence, conventional and asymmetric warfaring, and counterintelligence.

Variety Dynamics offers benefits in information warfare, particularly in efficiently and effectively changing the trajectory of ownership of power and control systems in hyper-complex situations. For example, Variety Dynamics:

- Can vary changes to the trajectory and ownership of power and control without needing to use force;
- Can operate covertly in complex and hypercomplex information warfare situations;
- Do not require expensive and hard to obtain causal information (this latter is especially expensive and difficult to obtain in information warfare situations);
- Have a potentially important role in asymmetrical information warfare;
- Offer better and faster prediction of outcomes than conventional analyses;
- Are relatively immune to misinformation and misdirection in counterintelligence;
- Have significantly lower costs than other approaches;
- Offer multiple informatic and physical pathways of application.

In hyper-complex information warfare situations, the distribution of variety of options available to different constituents is open to being influenced. As a result, the future trajectory of power and its ownership can be changed. In most information warfare situations, this can happen covertly.

Hyper-complex information warfare situations have archetypical structures, each of which aligns with different Variety Dynamics axioms that guide how best to influence the locus and to change the ownership of the flows of power and control.

Variety Dynamics builds on the earlier Law of Requisite Variety of W. R. Ashby (1956; Conant & Ashby 1970) and extends it with 47 axioms relating to changing the locus of power and control via changes in the distribution and dynamics of variety.

Variety Dynamics Axiom 1 explicitly extends Ashby's Law of Requisite to more complex situations.

Variety Dynamics Axiom 1

For complex and hyper-complex situations involving multiple constituencies in which the

distributions of variety generation and control variety is uneven across the system at any

one time, THEN

The differing distributions and dynamics of generated and controlling variety result in a structural basis for differing amounts of power and hegemonic control over the structure, evolution, and distribution of benefits and costs of the situation by different constituencies.

In short, Axiom One of Variety Dynamics states that control of a situation, and the distribution of benefits from it, depend on the structural distribution of varieties and changes to that distribution.

Put another way, Axiom One of Variety Dynamics describes how, by modifying the distribution and or dynamics of varieties in a situation, one can change the locus of power and control between constituencies. In information warfare terms, specifically, deliberate modification of the distribution and/or dynamics of variety in a situation enables one to change the trajectory and locus of control, and the distribution of ownership of control and benefits, towards preferred constituencies.

Basic examples of the above Variety Dynamics axiom include the use of a war dialler to use up a competitor organisation's resources, or the use of a DDOS attack with the same purpose. In commercial settings, business organisations manage their functions by passing information internally, and between themselves and customers and suppliers. A war dialling attack by one company against a competitor would be, for example, to continually dial (say) the sales desk such that it degraded the ability for the attacked company to compete. In Variety Dynamics terms, the attacking company increased the variety faced by a control system of the attacked company to reduce its control. Thus, the locus and ownership of competitive power and the distribution of benefits flowed towards the attacking company. The Variety Dynamics analysis of DDOS (denial of service) attacks on computer servers is similar.

Currently, Variety Dynamics research by the authors has led to more than 47 axioms identifying strategies to modify the trajectory of ownership of control in a variety of circumstances.

Example: Using Variety Dynamics Axiom 1 for Control of the Use of Improvised Explosive Devices (IEDs)

A practical warfaring example illustrating Variety Dynamics Axiom 1 is in responding to the use of improvised explosive devices (IEDs) against vehicles.

There are several different kinds of variety involved in the design, production, and use of IEDs, for example:

- Variety of designs of IED device as a package
- Variety of designs of ignition
- Variety of choices of explosive
- Type of vehicle target
- Type of location
- Variety of choices of laying the device
- Variety of purpose in using IED
- Variety of organisations using IEDs

Together, in any situation, the specific elements of the above list can be seen as a 'distribution' of

variety available to attackers who wish to use IEDs.

Those wishing to prevent or control the use of IEDs have a different distribution of variety: of strategies for intervention. This latter distribution of variety is of different controlling strategies that act to prevent the design, manufacture, placement, functioning, and or outcomes of IEDs.

The overall variety situation at any one time comprises the combined dynamic distributions of the varieties of the IED-using attackers and the varieties of those wishing to prevent changes in these patterns.

It is deictically obvious the scope and distribution of variety of those intending to control the use of IEDs must be larger than the practical scope and distribution of variety available to those wishing to use the IEDs.

If not, the range of options for those using IEDs will not be completely countered by those trying to control them, and IED use cannot be controlled.

Variety Dynamics Axiom 1 provides the basis to identify potential strategies to reduce the risk from IEDs and transfer the power and control towards the defenders.

There are several obvious large-scale potential variety-based strategies derived from Variety Dynamics Axiom 1 in this case:

- Increase the variety to be faced by those building and deploying IEDs. Examples include a) Saturate the control systems by which IED deployers control how defenders identify IED manufacture and deployment. This can be done by using different forms of investigation applied randomly on different targets; b) Use different forms of IED detection applied differently in different locations at different times; c) Vary attacks on IED production across different material supply chains, store depots, bomb makers, management paths, bomb components, and bomb targets. The aim is to increase the IED deployer's transactional costs and resources needed to protect the IED construction and deployment process by increasing the variety it faces.
- Attenuate the variety available to IED makers and deployers. This path is often seen as the only path by defenders as it can be most easily (though expensively) be implemented by force. It includes reducing the number of bomb makers, reducing access to IED making materials, reducing access to IED placing locations, and reducing cover for those placing IEDs. There are, however, many other options in attenuating variety.
- Increase the variety of other possible solutions to achieving the aims currently intended to be achieved through the use of IEDs. For example, in Afghanistan one of the key factors driving resistance to U.S. occupation was strong local concern about lack of access to traditional legal systems and courts. In many places prior to the U.S. military departure, such traditional courts were provided or enabled by Taliban services. In general, motivation to manufacture and deploy IEDs was in order to achieve specific aims because the variety of options available to progress towards achieving those aims was insufficient. Increasing the variety of alternative pathways reduces the relative power of attempts to achieve control via IEDs.
- Attenuate variety by gaining ownership or control of the supply chains for IED components, such as introducing additional varieties of component characteristics such that this requires IED deployers to develop different manufacturing techniques. The delay and testing and future variety of manufacture all result in increase in transaction costs and degrading the efficiency of IED manufacture and deployment, thus transferring power and

control away from the IED deployment.

Note that in a simple case, such as the above, identifying practical avenues is straightforward. Focusing on changing variety, however, exposes many other potential strategies that would be otherwise overlooked when the situation is viewed only via the lenses of force or direct causal control.

Example: Using Variety Dynamics Axiom 2 in Environmental Activists vs Motor Industry

Axiom 2 of Variety Dynamics focuses on the most basic changes of the locus and ownership of control in simple asymmetric situations:

For complex and hypercomplex systems involving multiple constituencies, some with more power and control,

THEN

If less powerful parties increase the variety faced by the more powerful parties, power flows from the more powerful parties to the less powerful parties and vice versa.

The underlying variety mechanism is that all organisations comprise both a system of generating variety and a system of control that reduces variety internally and externally.

Usually, for functional organisations, the ability of the controlling system to control variety exceeds the variety (internal and external) that the organisation is exposed to. The ratio between the controlling variety and the variety to which the organisation is exposed to is a measure of the power of the organisation. As that ratio decreases, the organisation loses power. By increasing the amount of variety to which an organisation is exposed, others can reduce its relative power. This power and potential for control flows to others.

In this example, environmental activists asked the motor industry to establish a vehicle emissions limit nationally. The motor industry refused and expected to use their significant wealth, power, and lobbying ability relative to the activists to be able to dominate them and the national government to guarantee to win out against the activists and ensure the motor industry wishes prevailed.

Following this refusal by the motor industry, the environmentalists undertook information warfare against the motor industry by increasing the variety to be faced by the motor industry. They did this by asking different states and countries to establish a variety of different emission standards. Some did so and some did not. The effect was the environmental activists significantly increased the external variety that the motor industry would face. The motor industry would then have to manufacture, and have certified, different variants of the same vehicle models for different states and countries. Not only would this add significant manufacturing and administrative burdens, but it would also mean that manufacturers and motor dealers would not be able to move or sell vehicles easily across boundaries without recertification and physical modification.

The result was the motor industry capitulated and agreed to a single national emissions standard.

The environmentalists were able to use their ability to increase the variety that the motor industry was exposed to the point where it exceeded the internally available control variety of the motor

industry and significantly increased their internal transaction costs and manufacturing costs together with the costs of their partners in the supply chain.

The result was a transfer of power from the motor industry to the environmental activists as well as achievement of the environmental activists' goals.

Example: Use of Variety Dynamics Axiom 14 in Explaining Terrorists' Use of 'Time-Related' Information Warfare Variety to Change the Locus of Power in an Asymmetric Context

Time is a dimension of variety in shaping the dynamic locus of power between constituencies in a situation. Variety Dynamics Axiom 14 describes this as follows,

The availability of system variety and control variety is dynamic and dependent on time.

THEREFORE,

Introduction of variety that results in changes to the time dynamic of availability of variety results in changes to the locus of power and the distribution of benefits and costs, of and to, different constituencies.

In this example, the ability of U.S. Special Forces to exert power and control over terrorists was significantly reduced by the use of a low-cost information warfare input that increased the variety to which the U.S. military was exposed and had a time-related effect on power and control. The outcome was a flow of power and control to the terrorists from the U.S. military.

It was reported that

> In March 2006, U.S. special forces conducted a successful operation. Less than one hour later, Jaish al-Mahdi (the group victim to the operation) released a video purportedly showing its soldiers had been executed whilst at prayer by the U.S. special forces soldiers. The U.S. military took three days to respond and also grounded the special forces battalion until the investigation had been completed—30 days later. A small terrorist organisation therefore executed a successful IW operation which tied up the U.S. government for 30 days. (Wilson 2022)

The disinformation video released by the terrorist group was a low-cost and zero-force way of introducing additional information warfare variety acting against U.S. Special Forces. It had significant time-related effects that reduced the potential variety of the U.S. Special Forces controlling response. It additionally caused time-related effects (Special Forces were stood down temporarily for a month) and caused significant additional transaction costs for both the U.S. Special Forces' information control system, and for the internal control system of U.S. Forces' management. The consequence was a transfer of the locus of power away from U.S. Special Forces and towards the terrorist group.

In this case, the terrorists' use of a disinformation video, Variety Dynamics analysis, rather than causal analysis, reveals that the terrorists could instead have increased the variety to which the U.S. military is exposed in many other different ways that would also have had time-related or other effects that would similarly have resulted in degrading the variety available to the U.S. forces to deliver power against the terrorists. There are many different low-cost variety-increasing opportunities available to terrorists that use information warfare rather than force. These include,

for example, information resulting in changes to military supply chains; honeypot or drug-related scenarios; communications creating internal tensions in U.S. forces; and attack misdirection, for example.

At this point in its development, the field of Variety Dynamics comprises a suite of Variety Dynamics axioms and concepts on how best to change the locus of power in hyper-complex situations such as information warfare. In parallel, these give rise to new bodies of theory in the fields of Systems and Management.

More abstractly, the concepts and principles of Variety Dynamics have led to a new body of mathematics that links to hyper-complex vector concepts and heterogenous, topological approaches to complexity that are emerging as an alternative to conventional AI/ML/transformer methods, such as GenAI and ChatGPT. This offers future potential for developing computational support for the use of Variety Dynamics in decision support in information warfare. Mathematically, Variety Dynamics appears to have three important properties a) it is theoretically decomposable (you can work backwards to find the underlying reasoning behind interventions); b) hyper-complex vectors are estimated to use significantly less computing power and energy (estimates at around 1/25th) and are faster in AI terms than more established approaches.

Conclusion and Summary

Variety Dynamics appears to offer significant advantages in information warfare both in attack and defence. Variety Dynamics has application in relatively straightforward information warfare situations alongside other approaches, usually causal in nature. However, the primary advantages of Variety Dynamics are in complex and hyper-complex information warfare situations. This is because Variety Dynamics helps address the limitations of other approaches in these realms.

Complex information warfare situations are those whose consequences are created by two or more feedback loops and following the Two Feedback Loop limitation Axiom are beyond the ability of humans to mentally predict consequences. This means that individuals or teams in information warfare are both unable to mentally predict the consequences of their decisions and at the same time have the mental delusion that they can do so. Both are implicated in adverse information warfare outcomes and present a limitation on using mental predictions as the basis for decision making in information warfare. Hyper-complex information warfare situations are those that, in addition to being complex, have structures and information architectures that do not conform to the assumptions required of systems' thinking approaches. This means that prediction of consequences from decisions and interventions is not only beyond the mental ability of humans, but such prediction is also outside the ability to address these issues using systems thinking methods and mathematical and process tools of systems analysis that require systems assumptions to be observed. This presents an additional limitation of use of information warfare decision-making methods for situations that do not conform to the assumptions of systems thinking and similar approaches.

Variety Dynamics addresses the above two limitations in information warfare by providing a different kind of forecasting of outcomes. In fact, the use of the concepts and axioms of Variety Dynamics goes beyond forecasting. Variety Dynamics provides direct, easily understandable guidance and reasoning for information warfare decision making aimed to favourably influence the location, trajectory, and ownership of power and control in a situation by changing the distribution and dynamics of variety. This then enables future control of outcomes.

Perhaps more importantly, the effectiveness of Variety Dynamics strategies in information warfare

can be more powerful than using force, typically does not require force, and also can support the use of force. Additionally, Variety Dynamics' adjustments of variety in situations are typically low-cost or zero-cost. Also, in complex and hyper-complex situations, Variety Dynamics interventions are in many cases naturally covert because of the Two Feedback Loop limitation constraint on humans mentally understanding the behaviour of situations.

In conclusion, the above suggests there is significant potential to use Variety Dynamics to extend the range and effectiveness of conventional information warfare practices, theories, and tradecraft.

Future research on Variety Dynamics will involve working with information warfare professionals to identify the most effective approaches to using Variety Dynamics in the field. Future research will be aimed at creating a body of practical examples of the use of Variety Dynamics in information warfare to develop additional practical guidelines and concepts that provide training material for the ongoing use of Variety Dynamics to effect changes in power and control.

References

Alberts, DS 1996 *Defensive Information Warfare*, National Defense University, Washington, D.C., US.

Ames, RT 1993, *Sun-tzu: The art of warfare: The first English translation incorporating the recently discovered Yin-chI\0300u\0308eh-shan texts*, 1st edn., Ballantine Books, New York, NY, US.

Ashby, WR 1956, *An Introduction to Cybernetics*, 2nd Impression, Chapman Hall, London, UK.

Betts, RK 1982, *Surprise Attack*, Brookings Institution Press, Washington D.C., US.

Bingle, M 2023, 'What is Information Warfare?', viewed 19 February 2025, <https://jsis.washington.edu/news/what-is-information-warfare/>.

Brooker, C 2021, *The Effectiveness of Influence Activities in Information Warfare. Australian Army Occasional Paper No. 8*, Australian Army Research Centre.

Buschman, TJ, Siegel, M, Roy , JE & Miller, EK 2011, 'Neural substrates of cognitive capacity limitations', *Proceedings of the Nationalal Academy of Sciences of the United States of America*, vol. 108, pp. 2711252-5, <https://doi.org/doi: 10.1073/pnas.1104666108>.

Conant, RC & Ashby, W R 1970, 'Every good regulator of a system must be model of that system', *International Journa of Systems Science*, vol. 1, no. 2, pp. 89-97.

Congressional Research Services 2018, *Information warfare: Issues for Congress*, Library of Congress, viewed 19 February 2025, <https://www.everycrsreport.com/files/20180305_R45142_c92c6be5763f84c05aee8a79ebe1727814d8da8d.pdf>.

Cronin, MA, Gonzalez, C & Sterman, JD 2009, 'Why don't well-educated adults understand accumulation? A challenge to researchers, educators, and citizens', *Organizational Behavior and Human Decision Processes*, vol. 108, no. 1, pp. 116-30, <https://doi.org/https://doi.org/10.1016/j. obhdp.2008.03.003>.

Doyle, JK, Ford, DN, Radzicki, MJ & Trees, WS n.d., 'Mental models of dynamic systems', ed. Y Barlas, *System Dynamics*, vol. II, UNESCO Encyclopedia of Life Support Systems, Paris, France.

Ekelhof, M & Paoli, GP 2020, *The human element in decisions about the use of force*, viewed 19 February 2025, <https://unidir.org/files/2020-03/UNIDIR_Iceberg_SinglePages_web.pdf>.

Engstrom, J 2018, *Systems Confrontation and System Destruction Warfare. How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, Rand Corporation, Santa Monica, CA, US, viewed 19 February 2025, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf>.

Forrester, JW 1972, 'Understanding the counter-intuitive behaviour of social systems', *Systems Behaviour,* Harper & Rowe Ltd., London, UK, pp. 270-87.

Grother, P, Ngan, M & Hanaoka, K 2019, *NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic effects*, NIST, Gaithersburg, MD, US, viewed 19 February 2025, <https://doi.org/10.6028/NIST.IR.8280>.

Hung, T & Yen, C 2023, 'Predictive policing and algorithmic fairness', *Synthese*, vol. 201, <https://link.springer.com/content/pdf/10.1007/s11229-023-04189-0.pdf>.

ICRC 2013, *The use of force in armed conflicts interplay between the conduct of hostikities and law enforcement paradigms,* ICRC, <https://www.icrc.org/en/doc/assets/files/publications/icrc-002-4171.pdf>.

Joint Chiefs of Staff 2022, *Joint Publication 3-0 Joint Campaigns and Operations*, US Department of Defense, <https://www.dau.edu/sites/default/files/webform/documents/25566/JP%203-0%2C%20Joint%20Campaigns%20and%20Operations.pdf>.

Joint Forces Chiefs of Staff 2018, *Joint Concept for Operating in the Information Environment (JCOIE)*, <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830>.

Keane, MP & Thorp, S 2016, 'Chapter 11 Complex decision making: The roles of cognitive limitations, cognitive decline, and aging', *Handbook of the Economics of Population Aging*, vol. 1, pp. 61-709.

Krishnadas, D 2021, *Taken by Surprise: Study of Intelligence Failures*, Amazon Kindle.

Love, T 2009, 'Complicated and complex crime prevention and the 2 feedback loop law', eds. T Cooper, P Cozens, K Dorst, P Henry & T Love, *Proceedings of iDOC'09 'What's Up Doc' International Design Out Crime Conference's*, Design Out Crime Research Centre, <http://www.designoutcrime.org/ocs2/index.php/iDOC/2009/schedConf/presentations?searchInitial=L&track=>.

—2010a, *Can you feel it? Yes we can! Human limitations in design theory (invited keynote),* CEPHAD 2010, Copenhagen. Denmark, <http://www.dkds.dk/media/forskning/cephad/konference/planary%20sessions/PS%20Love%20v3%20CEPHAD2010%20DKDS.pdf>.

—2010b, ‘Design guideline gap and 2 feedback loop limitation: Two issues in design and emotion theory, research and practices, eds. J Gregory, K Sato & P Desmet, *Proceedings of the 7th Design and Emotion Conference 2010 Blatantly Blues*, Institute of Design and Design and Emotion Society.

—2018, *The 2 Feedback Loop Axiom and its Implications for OR, Systems Thinking and Wicked Problems in Planning and Crime Prevention*, OR60 Operational Research Conference, Lancaster University, Bailrigg, UK.

—2023a, ‘Two feedback loop limitation axiom: Why participatory systems methods fail and are inappropriate for complex systems problems', *Journal of the International Society for Systems Sciences,* viewed 19 February 2025, <https://journals.isss.org/index.php/jisss/article/view/4158>.

—2023b, ‘Using variety dynamics to take control of coercive systems’, *Operational Research Society Conference OR65*, University of Bath, Bath, UK.

—& —2007b, ‘Successful activism strategies: Five new extensions to Ashby’, eds. K Fielden & J Sheffield, *Systemic development: Local solutions in a global environment, ANSYS 2007 proceedings*, Unitech.

—& —2008, *Machiavelli with extra variety: Taking organisational power and control* systems, Thinking Group, Perth, Australia.

—& —2011a, *Digital ecosystems: Conceptual optimisation to manage complexity, interoperability and viability*, working paper, Love Services Pty Ltd.

—& —2011b, *Using variety analyses to improve educational sustainability and liveability,* working paper, Love Services Pty Ltd.

—& —2021, ‘Variety dynamics for operational research’, *OR63 International Operational Research Society Conference*, Southampton, UK.

—& —2023a, ‘Variety dynamics in defence and security’, *7th IMA Conference on Defence and Security*, Imperial College, London UK.

—& —2023b, ‘Variety Dynamics: A new body of systems methods and a new mathematical field for management of dynamically complex multi-actor systems’, *Journal of International Society of System Sciences*, viewed 19 February 2025, <https://journals.isss.org/index.php/jisss/article/view/4159/1257>.

—& —2024, ‘New military history: Using variety dynamics’, *Military History Consortium Conference*, Lancaster University, Bailrigg, UK.

Molander, RC, Riddile, A & Wilson, PA 1996, *Strategic information warfare: A new face of war*, RAND National Defense Research Institute, viewed 19 February 2025, <https://www.rand.org/pubs/monograph_reports/MR661.html>.

Palmer, T 2022, *Primacy of Doubt*, Basic Books, New York, NY, US.

Papachristos, G 2019, ‘System dynamics modelling and simulation for sociotechnical transitions

research', *Environmental Innovation and Societal Transitions*, vol. 31, pp. 248-61,

Pursiainen, C & Forsberg, T 2021, 'The cognitive limitations of rationality', *The Psychology of Foreign Policy*, Springer Nature, Cham, Switzerland.

Schmid, U, Ragni, M, Gonzalez, C & Funke, J 2011, *Cognitive Systems Research*, vol. 12, nos. 3-4, pp. 211-18, <https://pmc.ncbi.nlm.nih.gov/articles/PMC3131328/pdf/pnas.201104666.pdf>.

Shannon, B, McGee, Z & Jones, B 2019, 'Bounded rationality and cognitive limits in political decision making', *Oxford Research Encyclopedia of Politics*, <https://doi.org/https://doi.org/10.1093/ acrefore/9780190228637.013.961>.

Shipman, MD 1981, *Limitations of Social Research*, 2nd edn., Longman Group, London, UK.
Simon, HA 1957, *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*, 2 edn., Macmillan, New York, NY, US.

Sterman, J 2006, 'Learning from evidence in a complex world', *American Journal of Public Health*, vol. 96, pp. 505-14, <https://doi.org/https://doi.org/10.2105/AJPH.2005.066043>.

—2018, 'System dynamics at sixty: The path forward', *System Dynamics Review*, vol. 34, pp. 5-47, <https://sdjournalclub.mit.edu/sites/default/files/documents/Sterman-2018.pdf>.

Sterman, JD 1989, 'Modeling managerial behavior: Misperceptions of feedback in a dynamic decision making experiment', *Management Science*, vol. 35, no. 3, pp. 321-39.

—1991, 'A skeptic's guide to computer models', eds. GO Barney, WB Kreutzer & MJ Garrett, *Managing a Nation: The Microcomputer Software Catalog*, pp. 209-29, Westview Press, Boulder, CO, US.

—2002, 'All models are wrong: Reflections on becoming a systems scientist', *System Dynamics Review*, vol. 18, no. 4, pp. 501-31, <web.mit.edu/jsterman/www/All_Models_Are_Wrong_ (SDR).pdf>.

—& Sweeney, LB 2007, 'Understanding public complacency about climate change: Adults' mental models of climate change violate conservation of matter', *Climatic Change*, vol. 80, pp. 21338, <https://doi.org/https://doi.org/10.1007/s10584-006-9107-5>.

Sweeney, LB & Sterman, JD 2000, *Bathtub dynamics: Initial results of a systems thinking inventory*, MIT, Cambridge, MA, US, <https://web.mit.edu/jsterman/www/Bathtub.pdf>.

US Department of Defense 2022, *Naval Doctrine Publication 1 Naval Warfare*, viewed 19 February 2025, <https://cimsec.org/wp-content/uploads/2020/08/NDP1_April2020.pdf>.