

NETWORK-CENTRIC INFORMATION POLICY¹

Professor Newton Howard

Center for Advanced Defense Studies (CADS)
Cyber Security Policy & Research Institute (CSPRI)
Department of Computer Science
The George Washington University
Phillips Hall
Washington, DC 20052
newtonh@gwu.edu

Ammar Qusaibaty

Université Paris-1 Sorbonne
17, rue de la Sorbonne
75005 Paris, France
amm.qusaibaty@malix.univ-paris1.fr

ABSTRACT

As information technologies continually produce mobile, decentralized, data systems, measures must be in effect to shelter assets from exposure to information warriors. A fundamental countermeasure to shield organizational data assets from attacks and provide information assurance is the development, implementation, and maintenance of an information policy (IP). IP can be characterized as a combination of finite and deterministic rule-based and case-based algorithms that regulate informational flow among different components in a defined network. Formal, IP research and methodologies are not widespread. As a result, this paper proposes three drivers, six dimensions, and various models to guide the cognitive processes of IP designers.

MAJOR POINTS

The primary focus of this paper is a discussion of the main aspects of an IP—drivers and dimensions. The interrelated relationships between IP drivers and dimensions are analyzed and accordingly viewed through models such as C3I3K (Command, Communication, Control, Intelligence, Intent, Information, and Knowledge) and 5WH (Who, What, Where, When, Why, and How). Moreover, the mutual impacts and influences between IP and society are examined in order to usher the applicability of IP out of the information technology (IT) sector into the higher realm of global governance as exemplified by the global informational economy.

1. INTRODUCTION

¹ Network Centric Information Policy is a working draft authored by the Center for Advanced Defense Studies (CADS). The National Security Agency (NSA) and Information Assurance Grant 2003 sponsor CSPRI-CADS' research.

** Published The Second International Conference on Informatics and Systems March 6-8, 2004

***Research support and edited by Olivia Goldschmidt and Zuri Kemp

Information policy (IP) is an advanced strategy that supports goals of organizational procedures and provides a proposal for maintaining the usability, integrity, confidentiality, and availability of data [Barman 02]. Moreover, IP is a form of control implemented through a set of procedures to confine, prevent, normalize, or evaluate possible actions in an interactive network of concepts, people, and systems.

Once an initiative associated with global information societies realizing national, social, and economic goals [James 01], IP has expanded its applicability to now incorporate the constantly changing realm of information technologies. Why? The rapid growth of information technologies dictated a critical need for all-encompassing, “*flexible, dynamic and responsive*” information policies [Rowlands 91].

In the information technology (IT) sector, an interactive relationship exists between users, systems, and environments. Therefore, it is befitting to view the study of information policy through the lenses of the actor-network theory. Founded by Latour and Callon [Latour 87; Callon 86], the actor-network theory is an important conjecture in the sociology of technology and science. In Latour and Callon’s analysis, the world is seen as a network of actants²—humans and non-humans, such as artifacts and systems—connected by links and relations. Translations along links occur to maintain the network’s functionality. The network’s ability to auto-recruit actants that translate language and values is an inherent socio-technical mechanism that involves systematic compromises and coordinated projects resulting in systems. The overall process of translation and communication among actants generates power relations [Foucault 80], concentration, and asymmetry of information [Arrow 86].

In other words, information policies address the dynamic flow of information between dimensions and drivers. The interrelated dimensions of IP are financial, social, legal, administrative, cognitive, and spatiotemporal variables that are directly related to the drivers of IP—users, systems, and environments. Together the drivers and dimensions become the backbone of an IP because therein the interactive combination lies the potential for a perfect IP that will maximize an organization’s efficiency.

Organizations at strategic, operational, and tactical echelons all seek to design perfect information policies, but are willing to settle for an IP that tackles its vital needs. Therefore, as a multidisciplinary research, this paper proposes a quasi-quantitative framework to understand the dimensions and drivers of IP (see Appendix: IP Analysis Framework). This paper will

moreover demonstrate the resourcefulness of information policies when faced with the Dr. Jekyll and Mr. Hyde of information technologies—information assurance and warfare.

Information assurance and warfare are relatively new concepts—both relating to the premium price on electronic information—ushered in during the aftermath of the Internet’s debut. Via information warfare, resourceful intruders exploit data systems and subsequently use the acquired information as both a tool and a weapon. Information assurance, however, counteractively positions data systems on the offensive by employing methods that guarantee the confidentiality, integrity, and availability of records. Prior to the utilization of information policies, data systems were sitting ducks for information warriors. Furthermore, corporations had no established methods to neither protect information nor recuperate after a data breach. Conversely, information policies provide a level of information assurance since documented counter measures and procedures are in place to thwart the malevolent intents and attempts of information warriors.

The necessity for information policies predates the actual existence and mass usage of such policies. Numerous, pre-existing infrastructures—airlines, automakers, hospitals, banks, electric power networks, water supplies, and railroads—have long since transitioned to information storage and processing technologies that were lacking noteworthy security controls [Edwards 98; Straub 89]. The introduction of assurance and security procedures into those information storage and processing technologies has presented IP producers and users with a key problem—the difficulty in devising an IP without noteworthy IP research and models pertinent to sociotechnology. As a result, this paper will serve as a guide for IP producers and users facing the new challenges to IP as IT becomes a more important and integral part of everyday life.

2. SCOPE OF INFORMATION POLICY

IP has an extensive scope due its structural composition—multiple factors that operate at different levels with varying intensity. The interactions and the relationships between society and technology further define the boundaries of IP reach. Mansell and Wehn assert that IP is not just about computer-based technology; instead, “Good policy with regard to the building of the Information Society must rely not only on sufficient technical and material resources [...] and skills, but also be coherent with other societal policies” [Mansell 98]. IP designers, therefore, must consider heterogeneous components, including organizational, social, and technical elements, to guarantee that the purpose of a policy supports its function. Consequently, it is difficult

² The normally used term of actors in such an interactive network is “actant”.

to precisely define the scope of IP due to its diverse influences. For that reason, one of the main challenges that IP creators and users encounter stems from the multidisciplinary nature of the topic and the wide range of infrastructures and variables to consider. True to its multidisciplinary composition, IP has the intrinsic capabilities to extend its applicability to decentralized production, informational economy, and capitalism.

Through post-Fordist regimes of accumulation, production is de-localized, thus extending the spatiotemporal constraints beyond conventional means. The post-Fordist model, which emerged out of the work of French regulators Aglietta [79] and Lipietz [87], interpreted the crises of the 1970s and 1980s as a deconstruction of Fordist political economy—the prevailing economy framed by Keynesian welfare policies, mass production technologies, and mass consumption culture. No longer relying upon traditional localized boundaries (e.g. labor and resources), transnational corporations (TNCs) have expanded their production capabilities worldwide. Modular, decentralized production contributed to the need for innovative technologies and organizational networks that, in turn, gave rise to a novel type of management system whereby actors manage information. “Actor-Network theory posits that decisions are made after the alignment of interests of the involved actors takes place. The alignment of interests is one of the possible outcomes of the continuous negotiation process, in which the actors are involved” [Callon 86].

The regulation of information thus became a prevalent channel to amplify efficiency between control center and production facilities [Dicken 92]. Therefore, TNCs, transitioning to minimize costs, yet maximize efficiency, began increasingly relying upon inventory systems, subcontractors, part-time labor, and other information technologies to achieve the bottom line—maximum, yet affordable, information access and speed. Digitized information has zero marginal cost,³ thus making it the ideal product for consumption.

Garrett Hardin’s “Tragedy of the Commons” refers to the general problem of exploitation of public goods, and specifically of natural resources, by a growing human population.

Therein is the tragedy. Each man is locked into a system that compels him to increase his herd without limit—in a

world that is limited. Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons. Freedom in a commons brings ruin to all. [Hardin 68]

Often to the detriment of others, individuals act rationally in their own self-interest in order to maximize their satisfaction and consumption of a public resource. Along similar lines of reasoning, individual interests often conflict with what is in the best interest for the public good.

Digitized information, however, as an inexhaustible resource—no reproduction cost—is a counterexample to the “Tragedy of the Commons.” Information is a public good inasmuch as it is virtually free of access and available for consumption. In this respect, competition among individuals shifts from information consumption to information access and interpretation. Internet bandwidth illustrates competition for access speed, not access. Informational access and interpretation, as dictated by IP, will always remain, regardless of form—digital or otherwise—asymmetric *vis-à-vis* the “Tragedy of the Commons.” IP, as exercised by individuals formally and informally, governs access to information and its implication.

Essentially, the post-Fordist paradigm created a new supply and demand market for information and services. Due to the move toward technological means of production triggered by the rise of information technologies, there currently exists a realization of the resultant potential for productivity of a mature industrial economy. A global informational economy is a historically new reality that is distinct from a world economy—capital accumulation proceeds worldwide. It is only in the late twentieth century that the world economy was able to become truly global—possessing the capabilities to work as a unit in real time on a planetary scale—due to the pioneering infrastructure provided by the information and communication technologies. For the first time in history, electronic capital is managed in internationally integrated, financial markets working in real time; innovative information technologies permit resources to be instantaneously shuttled between economies [Castells 96].

The decentralization of markets moreover extended into global governance, notably with the Bretton-Woods institutions that behave as a networker, information source, and regulator to analyze and influence the World Bank and International Monetary Fund (IMF). International trade flow liberalization policies, such as those set forth by the North American Free Trade Agreement (NAFTA) and the World Trade Organization (WTO), or international monetary flow, such as that

³ Marginal cost, an economic term, refers to the change in total cost (or total variable cost) due to a change in the quantity of output produced by an economic agent (often the firm) in the short run. It indicates the change in total cost resulting from a given change in output quantity. Mathematically, the term may be computed as the change in total cost (or total variable cost) divided by the change in output.

advocated by the International Monetary Fund (IMF), suggest modern, global modes of regulation also applicable to the post-Fordist regime of accumulation.

Although there existed an international need for a decentralized, informational economy, the rapid expansion of information technologies has propelled a growing marginalization of developing countries. Technologies such as the Internet maintain a potential of perpetuating a new type of cultural imperialism. Since this new supply and demand market for informational services was created in the developed world from a natural progression of production regimes, its technological applications are not profitable and often not appropriate in developing countries. The informational services are at an extreme disadvantage with the sociopolitical, economic, and cultural conditions in developing countries for one simple reason—Whereas basic needs are still unsatisfied in certain developing countries, developed economies impose their hegemony by dictating new needs reliant on informational technologies.

Conversely, on a smaller geographic scale, technological innovations possess the unleashed potential to bridge gaps between underprivileged communities, as illustrated by counter-hegemonic uses of the Internet. Notably, public agencies, through the Internet, “legitim[ize] and sustain existing ideologies and politics as normal, necessary, or natural [Warf 97]. In a trend to counter global capitalism, a greater coordination of localities has emerged. Informational networking can help establish stronger social relations, such as international alliances, through regulated access to information.

The current state of informational networks furnishes a fundamental foundation for the establishment of a nomadic power.

A diffuse power, with no location, [...] it maintains its autonomy through movement. Its valuables, electronic capital and electronic information, are located both nowhere and everywhere and cannot be physically captured. Nomadic power is not easily put on the defensive or defeated if it cannot be located. [Warf 97]

Therefore, only nomadic types of electronic resistance (e.g. information assurance) can counter elites—those reaping the supreme benefits—of this power system. However, the danger embedded in nomadic forms of electronic resistance revolves around the X-factor: Exploitation—entities receiving the information may only react/respond to that which caters most to their own set of belief systems.

3. DRIVERS AND DIMENSIONS OF INFORMATION POLICY

Another primary dilemma encountered by IP designers resides in defining the identities of IP drivers and dimensions in a typical actor-network theory scenario. In special scenarios, tailored IP drivers and dimensions are identified after the alignment of interests of the involved actors assessed by IP designers [Callon 86; Callon 89; Latour 93]. IP drivers are, in essence, the propellers or executors of a policy, and IP dimensions are both internal and external sources that influence the design, implementation, and maintenance of a policy.

On a basic level, IP is typically employed through three, interconnected drivers: environment, technology, and users (see Figure 1: The Drivers of Information). The environment driver takes into account the physical environment, as well as the surrounding social, legal, administrative, and cognitive environments. The technology driver focuses on the in-house technology that will ultimately control the functionality of the IP. The users are those having any interaction, either direct or indirect, with the IP or the information managed by the IP. In order to fully comprehend the roles and responsibilities of IP drivers, it is beneficial to review Herbert Simon’s synopsis of “symbol systems” and their relationship to informational flow.

IP is directly associated with the flow of information among “symbol systems”, or what is commonly referred to as information processing systems, computers, and people. The computer is not a singular technological invention but is instead a set of technologies driven by software applications with information processing resources [Landauer 95]; software applications make one physical machine infinitely many virtual machines. Consequently, Simon views computers as members of an important family of systems—“symbol systems”—because of their physical and virtual machine traits [Simon 96].

According to Simon, another important member of this family is the human brain and mind. The brain is the physical machine made of flesh and blood that correlates to the computer’s fabricated glass and metal hardware; the human mind is the virtual machine made of cognitive processes that parallel the computer’s software applications. “A symbol system is a machine that, as it moves through time, produces an evolving collection of symbol structures that serve as internal representations of the environments to which the symbol system is seeking to adapt” [Simon 96]. As a result, a symbol system must have means to:

1. Collect information from the external environment;
2. Encode the external information into internal symbols;

3. Manipulate internal symbol structures through reasoning procedures; and,
4. Produce symbols that initiate action in the environment.

Fundamentally, the basic abilities of symbol systems are therefore based on the collection, reorganization, production, and exchange of information. IP, from a symbol system perspective, deals with the flow of information from virtual infrastructures—human minds and software applications—to command & control physical infrastructures—human brains, machines, systems, and networks.

The three drivers—environment, technology, and users—do not operate independently but rather respond to each other in dimensional, interwoven networks; basically, the drivers function within power or force relations termed dimensions. Social, financial, administrative, spatiotemporal, cognitive, and legal variables comprise the dimensions of IP. While these dimensions have been divided for examination, they are all interrelated and often elements of one dimension directly influence another dimension.

The social dimension takes into consideration the attitude and acceptance of the policy by those having to interact with it. IP designers ought to be conscious of what people will render acceptable & necessary or unacceptable & unnecessary.

The financial dimension examines the fiscal motivators and ramifications of IP. Analysis must be done to determine the potential financial concerns in the development, maintenance, and enforcement phases of a policy.

The administrative dimension involves the managerial and clerical aspects pertinent to the policy's enforcement and maintenance. If there is a hierarchical security structure, this dimension moreover must take into account the current IP.

The spatiotemporal dimension appraises the actual physical time and space of the developmental aspects of an IP, as well as the policy's maintenance. The physical time and space dimension is important to examine mainly because information policies govern objects that often are accessed online, thus implying that the normal physical rules of access to such materials must be redefined.

The cognitive dimension revolves around the individual assessment of the IP by each user. The financial, social, legal, administrative, and spatiotemporal factors uniquely affect each entity. The cognitive dimension therefore analyzes each individual's reaction to the IP, which, in turn, directly influences the success and functionality of any policy.

The legal dimension explores the legality of a policy within the constraints of corporations, societies and

governing bodies. Consideration should be given to the differences between the set of laws governing the IP creators and the laws managing the IP users.

For a practical, step-by-step guide to assist in accounting for the variables associated with drivers and dimensions, the appendix—IP analysis framework—leads IP designers through the multi-phase process. After completing the phases, IP designers will be equipped with essential information—drivers, dimensions, amities, threats, and system options and constraints—about the system to be safeguarded. The identification of such variables will allow designers to reenter the planning phase and accordingly adjust control mechanisms. Most importantly, via referencing and applying the steps of the IP analysis framework, IP designers will have transitioned from the theoretical, planning phase of IP to setting the plan in action.

4. RELATIONSHIP BETWEEN DRIVERS AND DIMENSIONS OF INFORMATION POLICY

The principal IP drivers and dimensions often interact in such relationships that result in the creation of derived drivers and dimensions. Exemplifying such a relation, the social and legal forces intermingle, exert their respective influences, and create a derived dimension—transparency. Transparency, denoted in this work by “F1”, can be viewed as an intersection of the social and legal dimensions: $F1 = D1 \cap D6$, as illustrated in Figure 2 (The Derived Transparency Dimension).

Appropriately, transparency is the ability to see through systems and relational networks. An example of transparency is the degree of discretion and personal privacy granted by information policies. Basically, on a horizontal echelon, IP users feel that informational transactions are confidential, but if those same transactions were viewed on a vertical level, low-level users would then realize that higher-level users, hence upper echelons, are able to access all of the supposed private communications.

Unlike the derived dimension transparency, other resultant elements of IP may not manifest through predictable methods such as relational action. Therefore, IP designers must reference various models predictive of actions in an attempt to maximize the applicability and functionality of information policies. The 5WH model is comprised of who, what, when, where, why, and how type questions. The purpose of such elementary, interrogative queries allows IP designers to truly get down to the basic shapers and motivators of an IP. The C3I3K (command, communication, control, information, intelligence, intention and knowledge) model aids IP designers because it increases situational awareness and assists in determining events in various settings. Therefore, the C3I3K model allows IP designers to speculate along the

lines of reasoning of the 5WH model and subsequently predict reactions to certain system stimulants.

McCann and Pigeau extract the prime concepts from the C3I3K model and assert the dominance of command and control (C^2) over communication, information, intelligence, intention and knowledge. McCann and Pigeau claim, “ C^2 is the establishment of common intent to achieve coordinated action” [99]. Building upon the latter assertion, command is naturally associated with authority, responsibility, initiative, courage, trust and leadership—all of which are human activities. Control, however, is connected to plans, procedures, rules, communicational protocols, software, and equipment—all of which are non-human characteristics [Christiner 01].

Regarding the functionality of an IP, C^2 has unequal, yet complementary roles: (1) Command initiates control, and (2) Command is capable of dynamically altering existing control structures and processes to suit the unanticipated needs and priorities of a particular policy [McCann 99]. As such, IP is a structure of control that restricts, regularizes, and/or appraises possible actions, either known or predicted, in the context of dimensions. Just as control is a tool of command, dimensions are the corresponding tools of an IP. Dimensions thus create a control structure for the policy, and, within constraints, the policy helps to realize organizational goals.

C^2 is also useful when referencing the theoretical concept of perfect IP—the change of command, with respect to the spatiotemporal dimension (see Figure 3: IP Action Balance), is equal to the change of control in time and space. As shown in the equation below, the rate of change in command and control are equal. Therefore, the ratio—where x is command, y is control, and dt is space and time—is constant and equals one.

$$\frac{dy}{dt} = \frac{dx}{dt}$$

$$\text{Consequently, } \frac{dy}{dx} = 1.$$

Accordingly, perfect IP is able to dynamically keep up with the changing dimensions at an equal rate, as displayed in Figure 4 (Perfect IP) by the line with a slope of one.

Similar to the dimensional influences exerted by C^2 , the cognitive dimension has the potential to distort the perception of the other dimensions. This problem is a general example of the intention instantiation problem—how should intention be converted into well-organized action that supports the original intention in the midst of many other driving forces? Each person, either IP designer or user, has his/her own perspective of social, financial, legal, administrative, and spatiotemporal

variables. Figure 5 (The Cognitive Dimension’s Effect on Users) illustrates users’ cognitive reactions to an IP.

Therefore, the collective result of those individual, cognitive forces may drive IP into operational dysfunction. As such, there is a latent inconsistency between cognitive forces in IP and IP actions. This possible irregularity is an inherent weakness of IP and consequently creates vulnerabilities in the system that IP is safeguarding.

Essentially, IP functions as an information assessor, but information warriors seek out system vulnerabilities, such as those caused by the cognitive force, and exploit those weak links to no end. In view of that, a network shielded by a potentially inconsistent IP is a safer domain than a network not governed by any IP. Moreover, if information warriors were able to penetrate a system running under a potentially inconsistent IP, the task of isolating the weak link and recuperating would not be too burdensome due to the infrastructural controls strategically positioned by the IP.

5. CLASSIFICATION OF INFORMATION POLICY

Apart from discussions relating IP to drivers and dimensions, IP is also directly associated with events. Rowlands asserts that IP not only shapes events, but also responds to events; therefore, IP is classifiable through events. For example, e-commerce policies are examples of proactive information policies because they largely develop as responses to rapidly changing technologies in online retailing and business. Policy amendments after a security breach exemplify reactive policies because the policy has to defensively respond to the attack and attempt to restructure controls in such a manner that the overall fortifications of the system are reinforced.

Rowlands additionally proposed that there is no such thing as a single IP, but rather policies that address certain levels. IP is distinguishable across three hierarchical levels—infrastructural, vertical, and horizontal, as illustrated in Figure 6 (Classifications of Information Policy). Infrastructural policies address the development of national and regional infrastructures required to support society. Vertical information policies tackle litigious issues such as education, tourism, manufacturing, and health. Horizontal information policies attend to broader aspects of society like freedom of information, tariffs & pricing, and governmental relationships with citizens, businesses, and academia [James 01].

6. CONCLUSION

IP is a suite of directives and procedures administering how an organization handles, shields, and apportions sensitive information. Throughout this article, the

extensive scope of IP has been stressed and reiterated in various forms. From the global, informational economy to event-driven information policies, the requisite for IP in present-day society is at an all-time high. IP is rapidly developing into an informational indispensable as societies rely more heavily on computers and telecommunications in daily activities. Operating at its most basic level, IP is a useful tool for those venturing to assure informational assets and thus ward off attacks by information warriors.

However, the effectiveness and efficiency of an IP is only as good as the original intent and structural identifications of drivers and dimensions. Without an intention and proper classification of drivers and dimensions, an IP is essentially futile—it is probably attempting to shelter the wrong properties; moreover, the implementation is inaccurate since the infrastructural controls and constraints were not appropriately aligned with the intention.

In essence, the designing phases of an IP are just as interactive as an IP's drivers and dimensions. In order to maximize an IP's applicability and effectiveness, designers must not create an IP in a vacuum—without the significant input of drivers and dimensions—because IP does not operate within the constraints of a vacuum. If designed and implemented correctly, IP has the potential to approach the bounds of perfect IP—the policy dynamically transforms as drivers and dimensions change—and thus render information technologies virtually unbreakable and inaccessible to information warriors.

6. FIGURES

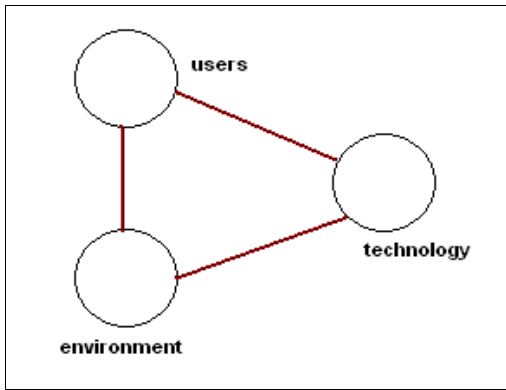


Figure 1: The Drivers of Information

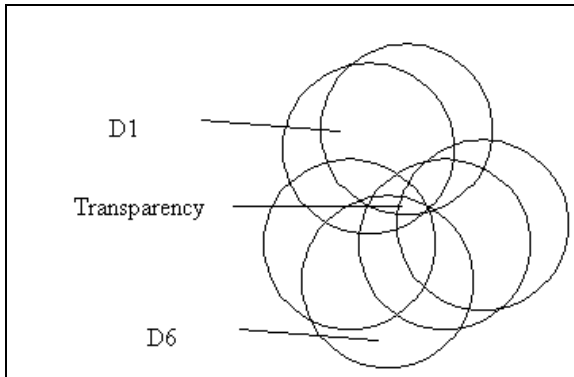


Figure 2: The Derived Transparency Dimension

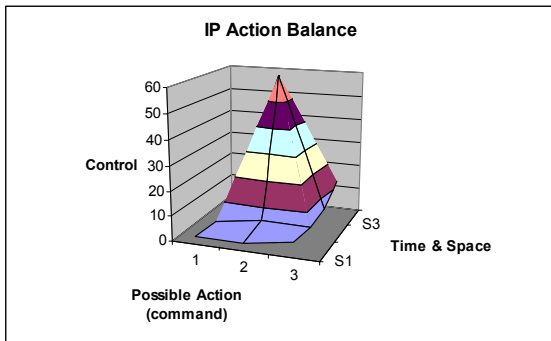


Figure 3: IP Action Balance

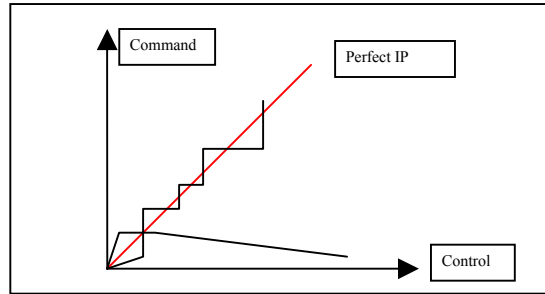


Figure 4: Perfect IP

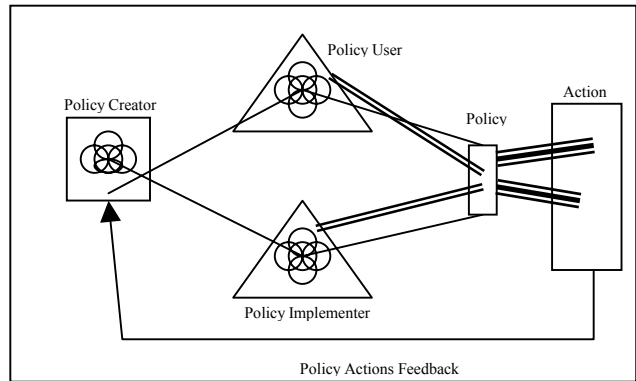


Figure 5: The Cognitive Dimension's Effect on Users

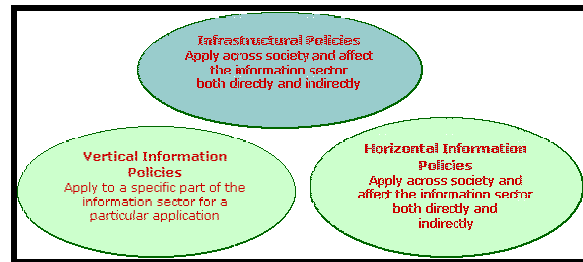


Figure 6: Classifications of Information Policy [Rowlands 91]

7. APPENDIX

Information Policy Analysis Framework

1. Every effective IP is based on intention. What are your organizational intentions?
2. Determine and define the environment to include technology and users.
3. Establish a scale—strategic, operational, or tactical.
4. Select an IP dimension—D1, D2, D3, D4, D5, or D6 (social, financial, administrative, spatiotemporal, cognitive, or legal)
5. Consider two classes of users in the environment according to intent—either friendly or hostile intentions. (One can extend the number of classes and follow a similar framework).
6. Calculate the size of classes C_f and C_h .
7. Assign positive values to classes C_f and C_h for friendly and hostile intention (v_f and v_h).
8. List system options and constraints for classes C_f and C_h in the same chosen dimension or other dimension of IP.
9. Assign positive values for options and negative values for constraints and add the ones of the same dimension. The sum of options and constraints constitute capabilities for friendly and hostile users.
10. Repeat steps 2, 4, 8, and 9 to refine information systems.
11. Calculate amities and threats based on the following equations:

$$\text{Amity} = \text{capability} \times \text{(friendly) intention}$$

$$\text{Threat} = \text{capability} \times \text{(hostile) intention}$$

12. Therefore,

$$\text{Amities: } \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$$

$$\text{Threats: } \theta_1, \theta_2, \theta_3, \dots, \theta_m$$

13. Multiply threats and amities with hostile and friendly class size respectively to evaluate actual amities and threats (one may consider subclasses in a class in relation to specific threats or amities). Then, consider the maximum values.
14. Let $\alpha = \max\{c_i \alpha_i\}$ and $\theta = \max\{d_i \theta_i\}$.
15. Calculate the dimensional balance ratio $\rho = \theta / \alpha$.

16. See Figure 7: Dimensional Balance. An information policy is a process for a balance ratio to converge to a perfect ratio and diverge from a failure ratio.

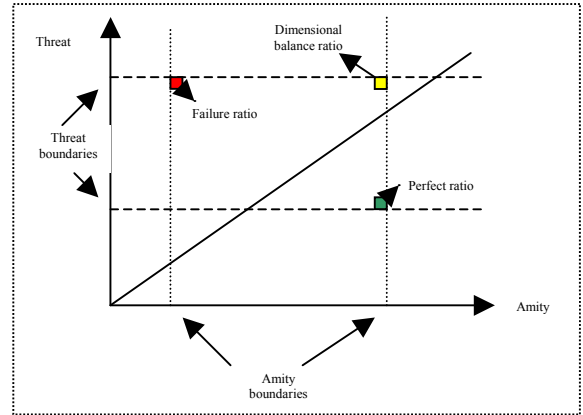


Figure 7: Dimensional Balance

17. Change options, constraints, intentions, and number of class members in relation to information systems and repeat the process.
18. Consider other dimensions and refine boundaries of threat and amity. See Figure 8: Multidimensional Balance.

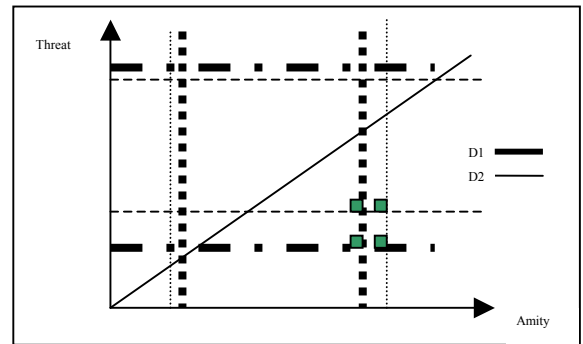


Figure 8: Multidimensional Balance

19. The strategy is to increase amity and reduce threat within the constraints and options of all related systems and users.
20. From the above analysis, it follows that there is a policy threat matrix and a policy amity matrix. The policy threat matrix is a 6x6 matrix whose entries are threats in one dimension in relation to all dimensions. The policy amity matrix is also a 6x6 matrix whose entries are amities in one dimensions in relation to all dimensions.

Policy Amity Matrix, $\Pi = \begin{bmatrix} \alpha_{11} & \alpha_{16} \\ \alpha_{61} & \alpha_{66} \end{bmatrix}$,

and,

Policy Threat Matrix, $X = \begin{bmatrix} \theta_{11} & \theta_{16} \\ \theta_{61} & \theta_{66} \end{bmatrix}$.

21. Metrics for an IP are matrix determinants for threat and amity matrices, $\det(\Pi)$, and $\det(X)$.
22. Calculate the determinant variation in time.

8. REFERENCES

- [Aglietta 79] M. Aglietta, *A Theory of Capitalist Regulation: The US Experience*, D. Fernbach, Trans., London: NLB, 1979.
- [Arrow 86] K. J. Arrow, "The value of and demand for information," in *Decision and Organization*, 2nd, C. McGuire and R. Radner, Eds., Minneapolis: University of Minneapolis Press, 1986, pp. 131-159.
- [Barman 02] S. Barman, *Writing Information Security Policies*, Boston: New Riders Publishing, 2002.
- [Callon 86] M. Callon, "Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St. Brieuc Bay," in *Sociological Review Monograph*, no. 32, *Power, Action and Belief: A New Sociology of Knowledge?* J. Law, Ed., London: Routledge and Kegan Paul, 1986, pp. 196-233.
- [Callon 89] M. Callon and J. Law, "On the construction of sociotechnical networks: Content and context revisited," *Knowledge and Society*, no. 8, pp. 57-83, 1989.
- [Castells 96] M. Castells, *The Rise of the Network Society. The Information Age: Economy, Society, and Culture*, vol. 1, Malden: Blackwell Publishers, 1996.
- [Christiner 01] Lieutenant-Colonel G. Christiner, "Command Versus Control in the Age of Information Technology." Advanced Military Studies Course 4: Canadian Forces College, 2001. <<http://198.231.69.12/papers/amsc4/christiner.doc>>.
- [Dicken 92] P. Dicken, *Global Shift: The Internationalization of Economic Activity*, 2nd, New York: Guilford Press, 1992.
- [Edwards 98] P. N. Edwards, "Y2K: Millennial reflections on computers as infrastructure," *History and Technology*, vol. 15, pp. 7-29, 1998.
- [Foucault 80] M. Foucault, *Power/Knowledge: Selected Interviews and Other Writings*, C. Gordon, Ed., C. Gordon et al., Trans., New York: Pantheon Books, 1980.
- [Hardin 68] G. Hardin, "The Tragedy of the Commons," <<http://www.sciencemag.org/cgi/content/full/162/3859/1243>>, *Science*, vol. 162, no. 3859, pp. 1243-48, 1968. (09-17-2003).
- [James 01] T. James, Ed., *An Information Policy Handbook for Southern Africa: A Knowledge Base for Decision Makers*, N. Butcher et al., Trans., Johannesburg: Hot Dot Print, 2001.
- [Landauer 95] T. K. Landauer, *The Trouble with Computers: Usefulness, Usability, and Productivity*, Cambridge: MIT Press, 1995.
- [Latour 87] B. Latour, *Science in Action: How to Follow Scientists and Engineers through Society*, Cambridge: Harvard University Press, 1987.
- [Latour 93] B. Latour, "Ethnography of a 'high-tech' case: About Aramis," in *Technological Choices: Transformations in Material Culture since the Neolithic*, P. Lemannier, Ed., London: Routledge and Kegan Paul, 1993, pp. 372-398.
- [Lipietz 87] A. Lipietz, *Mirages and Miracles: The Crises of Global Fordism*, D. Macey, Trans., London: Verso, 1987.
- [Mansell 98] R. Mansell and U. Wehn, Eds., *Knowledge Societies: Information Technology for Sustainable Development*, New York: Oxford University Press, 1998.
- [McCann 99] C. McCann and R. Pigeau, "Clarifying the Concepts of Control and of Command," in *C2 Decision Making and Cognitive Analysis*, D. Serfaty (APTIMA, Inc), Ed., presented at Command and Control

Research and Technology Symposium (CCRTS), United States Naval War College: Department of Defense Command and Control Research Program (DOD CCRP), 1999.

- [Rowlands 91] I. Rowlands and S. Vogel, *Information Policies: A Sourcebook*, Los Angeles: Taylor Graham, 1991.
- [Simon 96] H. A. Simon, *The Sciences of the Artificial*, 3rd, Cambridge: MIT Press, 1996.
- [Straub 89] D. W. Straub, Jr. and J. C. Wetherbe, "Information technologies for the 1990s: An organizational impact perspective," *Communications of the ACM*, vol. 32, no. 11, Nov., pp. 1328-1339, 1989.
- [Warf 97] B. Warf and J. Grimes, "Counterhegemonic discourses and the Internet," *The Geographical Review*, vol. 87, no. 2, Apr., pp. 259-274, 1997.