# Applying Principles of Reflexive Control in Information and Cyber Operations

ML Jaitner[1], MAJ H Kantola[2]

[1]*Swedish Defence University*
*Stockholm, Sweden*
*E-mail: margarita@csans.eu*

[2]*Finnish National Defence University*
*Helsinki, Finland*
*E-mail: harry.kantola@mil.fi*

**Abstract:** *According to Russian methodologies, the theory of Reflexive Control (RC) allows an initiator to induce an adversary to take a decision advantageous to the initiator through information manipulation. The RC theory encompasses a methodology where specifically prepared information is conveyed to an adversary, which would lead that adversary to make a decision desired by the initiator. The methodology is generally understood by Russian planners to be applicable in a wide variety of situations, and is deeply rooted within Russian Information Warfare concepts. Because theory envelops the Russian understanding of information as both technical data and cognitive content, 'information resources' are understood as technological as well as human. In principle, a well-developed (global) cyberspace presents theorists and operators of RC and RC methodology with numerous possibilities to affect their adversaries. This paper explores ways in which RC can be exercised with the help of the cyberspace.*

**Keywords:** *Reflexive Control, Cyberspace, Information Warfare, Cyber Warfare, Influence Operations*

*The quality of decision is like the well-timed swoop of a falcon which enables it to strike and destroy its victim.*
--Sun Tzu, *The Art of War*

## Manipulating Decision-Making

In an armed conflict or political struggle between states, one of the foremost tasks is to interfere with the adversary's decision-making process. One of the simplest taxonomies for decision-making processes is the subdivision into human-only, machine-only automated, as well as human machine assisted and collaborative decision-making systems.

In current military decision-making processes, the human machine-assisted process is most prevalent. Machine-only automated decision-making systems are currently still frowned upon (Kott 2015). While machines may be taking over more and more steps of the process, it is not likely that humans will disappear as decision-makers—even if their role might in the near future be reduced to simple oversight and emergency-stop functions. Therefore, this paper focuses on collaborative and machine-assisted decision-making systems. Two distinctive potential attack points can be identified in an environment of a human machine-assisted decision-making process. For one, the adversary can try to influence the human; and for the other, the adversary can try to influence the machine.

Modern decision-making processes emphasize the importance of recurrent gathering and evaluating of information, a comprehensive approach, in order to enable initiators to create Courses of Action (COAs) for their own actions, as well as models for their adversaries' COAs. In this way, COAs are, for the most part, based on intelligence and information provided by various Situational Awareness (SA) systems, weapons systems, and the like. Thus, decision- making processes rely heavily on collection of data that is purposeful, correct, and timely. Inaccurate and/or irrelevant information as well as delays in presentation can seriously cripple a decision-making process. In the context of human machine-assisted decision-making, this means that false, irrelevant, or untimely information can be introduced to the human, to the machine, or to both.

Arguably, decision-making processes follow certain patterns or logic. Such patterns can reside on various levels and may be technological as well as human. Within technological systems, the range stretches from simple warning systems that are triggered by a pre-programmed value, such as a conventional smoke detector, to complex systems that take a multitude of factors into account. In human decision-making processes, the patterns are constructed through human behaviour at the individual level, as well as at the group level. Such patterns are constructed through scores of factors ranging from cultural aspects and organizational structures to individual characteristics, such as the propensity to take risks amongst the decision-makers. In many cases, the complexity of such patterns increases along with the critical nature of the decision-making system. Thus, mapping of decision-making patterns may present an extremely challenging, but still achievable task. It is the knowledge of patterns within the decision-making process that allows an adversary to insert information into the process that would ultimately allow manipulation of the decision.

The aim of this paper is to explore how the theory of RC can assist in gaining an advantage over an adversary's decision-making process. First, the authors provide an overview of the theory of RC and exemplify its general use based on events in the near past. Then they describe three scenarios for manipulation of data. Each scenario is covered from two perspectives—cyber and cognitive-informational. Following these scenarios, the authors present a fictitious case, in which cyber and cognitive-informational manipulations are applied based on the theory of RC. Finally, they identify conclusions on the usability of RC in the context of Cyber and Information Warfare. In order to avoid confusion in terms of terminology, the following definitions will serve for the entire discussion: Information Operations include all operations that aim at cognitively interpreted information, whereas Cyber Operations in the first place aim at exploiting technological data, by, for instance, manipulating sensors or other Computer Network Attack (CNA) operations. The authors will also use the terms Information and Cyber Warfare in order to describe the manner of warfare, in contrast to delimited operations.

## Theory of Reflexive Control

The theory of Reflexive Control (RC) originated in the Soviet Union in the 1960s and has been more or less continuously developed ever since, with some of the original researchers in the area still actively engaged. Amongst the scientific founders of the theory are V. A. Lefebvre, who now resides and works in the U.S., V. E. Lepsky, associated with the journal *Reflexive Processes and Control* as well as the resource reflexion.ru, and also M. D. Ionov and S. Leonenko. The approach has its background in ideas established in the Far East such as the strategic thinking of Sun Tzu and particularly the Chinese use of stratagems. For example, Niu, Li and Xu (2000) emphasize ten stratagems to be used in Information Warfare.

RC can be defined as “a means of conveying to a partner or an adversary specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action” (Thomas 2004). The essence of a ‘reflexive game’ according to Lefebvre is found in the mutual attempts of the adversaries to impose RC over one another (Kramer *et. al*. 2003). This requires both adversaries to analyse their own ideas, and to model their adversary’s behaviour in accordance (Kramer *et al*. 2003; Thomas 2004). Reflexivity stands for the ability to create a correct model (Thomas 2004). The more accurate the model, the more precise will be the prediction of the adversary’s behaviour, the better will be the ability to introduce the desired ‘information package’ to the adversary.

In a military context, M.D. Ionov (1995) identifies four distinctive ways to introduce such an ‘information package’ to an adversary:

1. Applying pressure by show of force. Such show of force can be exercised in various forms stretching across different aspects from diplomatic or economic pressure, such as threat of economic sanctions to threats of military action, such as increasing combat readiness of armed forces or provocation to declarations of war.

2. Providing false information. This approach suggests the use of maskirovka—camouflage, denial, and deception—on all levels in order to manipulate the adversary’s perception of a situation. This includes showing great force where there is indeed a weakness and vice versa, as well as the use of Trojan-horse techniques.

3. Affecting the adversary’s decision-making process. Such approach includes systematic modelling of processes, publication of deliberately distorted doctrines, as well as presenting false information to the adversary’s system and to key figures.

4. Affecting the timing of decision. Here, the element of surprise might be employed by the sudden beginning of military operation or misleading the adversary to focus on another area of conflict to delay reaction.

The term ‘information’ should be understood in a broad fashion as it also includes emotional and controlling elements. Show of (military) force, for example, may not so much aim at presenting the size and equipment of troops, but rather serve to intimidate or to provoke an emotional reaction. At the same time, the information can also be introduced at machine level (Thomas 2004).

Identifying the weak link within the adversary's processes, the point at which the 'information package' can be introduced, is central to RC. Likewise, it is necessary to know what type of information needs to be included into the package. As Leonenko (1995) describes it,

> RC consists of transmitting motives and grounds from the controlling entity to the controlled system that stimulate the desired decision. The goal of RC is to prompt the enemy to make a decision unfavourable to him. Naturally, one must have an idea about how he thinks.

The various approaches to what is included into the notion of 'information' indicate the existence of two distinct layers of data that can become subjects of reflexive control. The first layer is constituted by the 'eyes, ears and noses'—or sensors of technical systems—that are used to gather values that describe a context or a situation. The actual processing of these facts, the sense-making, constitutes the second layer. This layer involves the cognitive aspect of human decision-making as long as a human in any way is involved in the process. It is the second layer that returns an actual understanding and knowledge of the situation or context (Thomas 2009). This in turn means that both these layers need to be taken into account when trying to apply the theory of reflexive control.

## Manipulating Data

Numerous ways to manipulate cognitive information and data exist. These range from withholding information or access to it, to providing an adversary with false information to create a deception, to flooding the adversary with information of varying significance.

Withholding information from an adversary is often a desirable technique to conceal friendly strengths, weaknesses, and plans. A general distinction can be made as to whether the adversary is aware of information being withheld. Particularly in cases where the adversary is unaware of an important information gap(s), the initiator can exploit this weakness.

In those cases in which the adversary is aware of, or at least suspects the existence of the withheld information, the action of concealment may be straightforward. In a more intricate approach, the fact that the information is hidden would be emphasized. This would force the adversary to focus efforts on uncovering the missing bit of the puzzle, potentially sending the adversary on a wild goose chase.

Leonenko describes the use of computers as a possible hindrance, since computer power can be used to calculate, model, simulate situations, and thus reveal the reflexive control attempt (Thomas 2009). However, in some cases, the opposite may well be the truth. Withholding data from information systems used to assist decision-making will affect the results that these systems return. The aim can range from bluntly disabling the decision support system to covertly forcing the system to present the adversary with false values; in the first case, the decision-maker would have to take actions based on insufficient information, potentially making decisions that are favourable for the adversary. In the latter case, where the manipulation is meant to stay covert, sound knowledge of the information system is required in order to be able to carefully choose information to withhold. Prior Information Warfare operations may be needed in order to make the value returned by the system believable to the decision-maker. Even in those cases where the value returned by the system appears incorrect to the human decision-maker, the adversary may gain an advantage by simply sowing distrust and confusion, which would, in particular, hamper decision-making in a fast-paced environment (Kott 2015).

In cyberspace, for example, withholding information can interfere with communication means (Chatham House). For instance, satellites are relatively vulnerable to external actions, since after their launch it is impossible to update the hardware while software updates are restrained by the overall architecture (Santamarta 2014; Hackett 2015). Activities may also include destroying information or parts of it in data centres, redirecting information searches to faulty sites, or overloading the system so that access cannot occur, for instance, through different versions of (R)DDoS attacks or by disabling sensors. Of course, decision-making in military contexts is mostly done in closed-circuit networks or in military-specific environments, which are often thought to gain access through cyberspace. This does not mean that withholding information is impossible, but it requires a substantial amount of planning and preparations in addition to actually gaining physical access to the network (Zetter 2015).

Information overload as a method is directly opposite to withholding information and "occurs when information received becomes a hindrance rather than a help when the information is potentially useful" (Bawden, Holtham & Courtney 1995). On the cognitive level, such an approach amounts to presenting the adversary with masses of information. Knowledge of the adversary allows tailoring loads of information in a way that would catch the adversary's attention. This way, decision-making can be stalled by the time the adversary needs to process or dismiss the information. Thus, the information must be of some potential value, or it could simply be ignored. It must also be accessible, or the overload will remain potential, not actual (Bawden & Robinson 2009).

Altering information can appear to be a more complex technique than withholding information. The benefit of this approach, however, is that it is often hard to detect. Gradually changing information will eventually alter the outcome of the analysis and thus direct the adversary's actions towards the desired end state (Kantola & Hämäläinen 2013). This applies at the cognitive level, such as information directed at decision-makers through open source channels, as well as at the machine level.

Altering information also has a higher reliability and predictability in terms of how the adversary will act. The challenge lies in the need to have a high-level insight into the system in question, aside from having access to it. Sufficient insight would include a technical understanding of how data is processed within the system. Further, a cultural and organizational understanding of how the human decision-makers analyse and interpret the values returned by the system is required. As in previously presented cases, prior application of Information Warfare might be necessary to 'prepare' the decision-maker to accept the values that the affected system would return. The manipulation is likely to be quickly discovered when a sudden change in results is presented by the system or when the system presents values that are inconsistent with the decision-maker's perception of the situation. With techniques, as described above, of withholding or altering information, distrust and confusion is likely to ensue. The level of distrust and confusion is highly dependent on the characteristics of the human decision-makers, including culture, overall trust in technology, existence of contingency plans, and other factors. Studies have shown that inaccurate information may present a greater problem than information denial, because inaccurate information affects the preconception of the situational awareness (Bryant & Smith 2013).

Increased use of Blue-force Tracking-type functionalities provides opportunities for efficient utilization of information altering techniques (Bryant & Smith 2013). Force tracking systems usually present both blue (friendly) and red (hostile) force information that is retrieved by manual entry as well as updates by a network of different sensors. This provides the adversary with a multitude of attack vectors to utilize reflexively (Thurston *et al*. 2013). Blue-force-tracking systems often use a standardized protocol for exchanging information, which makes it easier for an attacker to understand how to alter the information. Furthermore, such systems utilize an increasing number of various [weapon] sensors (Thurston *et al.* 2013), which multiplies ways to alter information provided to the decision-maker.

False or 'properly modified' information, including contradicting information, can be provided directly to the adversary via cyberspace for the use of decision-makers if a channel is established to their situational awareness system or made 'available' in suitable forums, databases, or information sources for pick-up into their own network. As previously noted, the values returned to the decision-makers should make sense to them; thus, simultaneously providing supporting information through other channels may be required. Similarly, compromising only one sensor system would in most cases remain insufficient.

## Case

In the previous section a number of techniques have been introduced, techniques following the principles of RC theory that can be used for manipulation of information on both the cognitive and on the machine level. This section will demonstrate how RC can be applied in a fictional operational setting. In this fictional scenario, neighbouring countries A and B are entangled in a dispute. Country B possesses significant cyber capabilities and has a tradition of applying RC in politics as well as on the battlefield. Both countries are aware of three strategically important areas on the territory of Country A (X, Y and Z), which Country B assesses to be desired points of attack. The access to each of these three areas is distinctive, as they are dispersed through the country on the north-south axis. Country B initiates an operation in five phases during which it will attempt to exercise reflexive control over Country A's military and political decision-makers.

> **Phase 1.** As the tensions between the two countries rise, Country B begins to prepare a military resolution of the conflict. B begins to mobilize troops and conducts exercises that can be perceived as targeting Area X. Country A's intelligence intercepts a number of leaked documents that point to imminent offensive action with Area X as a target. Country A's CERT and Cyber Defence Units also identify a significant rise in relatively small-scale attacks, which they can with relative probability link to hacktivist and cybercriminals with ties to Country B. Country B's media reports on mobilization, which Country A's reporters quickly pick up, which probably results in increasingly hostile chatter between the countries in social media.

**Phase 2.** The next phase of Country B's operation begins as documents are planted for Country A's intelligence service to find within the service's regular activity. The documents suggest that Areas X and Y are less suitable for an initial offensive from B's perspective. The discovery of these documents coincides with what A perceives as B's de-escalating at the highest political level. While B's troops remain mobilized, A's political arm attempts to engage in political resolution.

**Phase 3.** The third phase is initiated by Country B's sudden exercise that implies an imminent attack on Area Y. The exercise is widely communicated to media, and B actively encourages debate in social media regarding the details using 'trolls'/opinion agents. At the same time, B abruptly terminates diplomatic de-escalation. Country A's CERT and Cyber Defence Units identify increased small-scale cyber activity targeting the country's governmental and privately owned systems. Country A extends the high- alert level for troops despite the earlier indication that Y (as well as X) are less advantageous for B's offensive.

**Phase 4.** A brief period of de-escalation follows, during which Country B makes sure that the previously leaked documents regarding Area X and Y's unsuitability for B's offensive become widely known to Country A's civil society. For this purpose, B may want to activate analysts that have a history of supporting and propagating B's views in A's media. At this point, B utilizes any resource that may encourage A's society to terminate the state of high alert.

**Phase 5.** In the final phase of the operation, Country B attempts to give a credible impression of imminent attack against area Z. Country B chooses to simultaneously spoof Country A's military and civilian air surveillance systems, creating an impression of planes flying into certain bases adjacent to Area Z. Simultaneously B lets information surface regarding ground transports in the same direction. The aim is to create a perception of massive troop movement into that area—which also corresponds with the plans initially leaked during the first de-escalation in Phase 2. Ideally, this operation does not remain virtual; instead, it is supported by the actual movement of transportation trucks and trains toward the specified area in order to avoid discovery of the deception. In the event that case A's cyber intelligence is known to be able to collect information, fake plans and information could be planted for intelligence forces to collect or, if possible, even planted straight into its systems.

Cyber activities must be aimed at selected sensors, for example, the air surveillance system, as well as supporting information sources such as databases. Coordination with media reporting and other (planted) evidence is highly desirable, if not necessary. Social media offers a range of possibilities—troops available along the presumed transportation route can be encouraged to post pictures, geo-tag activities, and the like. Bots then can multiply this human activity in social media.

At this point, the previously provided false information of Area Z being the most favourable point of attack and the situational picture provided by sensors and systems for decision-making assistance converge. Public appearance, such as in media and social media, confirms the picture to Country A's decision-makers. At this point A's assessment of an imminent attack in area Z should be of such confidence that it triggers a defensive operation towards the area. At this point, the defensive operation at Area Z is likely to have public support.

The phase culminates as Country B launches an actual offensive in area Y, surprising Country A. Preparations for this activity would have happened during the previous phases on a low scale—from mobilization of troops in the initial phase, to preparing the actual offensive during Phase 3.

Activities in the different phases are summarized in **Table 1**, below.

According to the scenario, Country B applies the following methods in order to deliver the required information to Country A's decision-makers:

1. False information is being pushed into the adversary's systems and/or provided to be fetched by A's intelligence gathering routine (Phases 1, 2, 3, 5)
2. Information is being been altered in third-party/open systems (Phase 5)
3. Manipulated information is being provided to sensors (Phase 5)
4. Accurate information is concealed (Phases 1–5)
5. Mass-dissemination of information is being conducted (Phases 1–5)

An important element within the operation is the control over the consistency of overall information available to A's decision-makers and society. This allows Country B to create confusion, when the purposefully leaked false assessments do not correspond with actual mobilizations, in particular in Phase 3. This also allows Country B to evoke Country A's confidence in its situational assessment in the final phase, Phase 5. A confidence then leads to action based on the holistically manipulated situational picture. Thus, during the course of the operation, Country B establishes relative information superiority, which allows it, to a certain degree, to steer its adversary's reactions reflexively.

As previously noted this scenario is generic and aims to demonstrate as many of the manipulation techniques as possible. The variation of techniques that can be applied in an actual scenario may differ significantly depending upon numerous factors. Technological abilities, cyber readiness, level of skill of cyber-operation planners, and knowledge of the adversary are among these factors. Ultimately, each real situation will be unique and will require an individual solution.

| **Phase** | **Actor B** | **Actor A** | | |
|---|---|---|---|---|
| | | *Cognitive-informational activities* | *Cyber activities* | |
| **0**<br>**Initial stage** | Actors A and B are in discord. Actor B decides to resolve discord militarily. Three possible attack areas identified within Actor A's territory: X, Y Z. | | | |
| **1**<br>**Pressure and mobilization** | Mobilization of troops | Pressure against point X is promoted in media as well as through leaked documents | Low key supporting activity conducted by 'hacktivists' and cybercriminals | Threat perception at X, high alert with focus on X |
| **2**<br>**Planned planting and leaking of information** | De-escalation | Leaking of documents suggesting X and Y less suitable for attack, Z preferred | Planting of documents suggesting X and Y less suitable for attack, Z preferred | Attempts to engage in diplomatic resolution, acute threat perception eases |
| **3**<br>**Change of focus area** | Engagement in diplomatic resolution halts abruptly; Manoeuvres and simulations of attack against area Y | Pressure against point Y is promoted in media as well as in social media | Low-key supporting activity for the information campaign, employment of 'hacktivists' and cybercriminals | Tension rises, close observation, possibly inconclusive intelligence analysis |
| **4**<br>**Creating confusion** | Troops remain covertly mobilized towards Y; otherwise, de-escalation | Full scale promotion of area Z's higher suitability for attack than X, Y | Low-key supporting activity for the information campaign | Inconclusive intelligence analysis |
| **5 a.**<br>**Major deception** | Hide further mobilization towards B in the 'noise' | Clear and massive indication of troop movement towards Z in media & social media | Attack sensors supporting perception of troop movement towards Z | Sensor results support intelligence analysis; Troop concentration towards Z |
| **5 b.**<br>**Attack** | Attack at Area Y | | | |

**Table 1:** Informational activities during the five phases of the generic Reflexive Control operation

## Conclusions

This paper describes how cognitive information and cyber operations can be manipulated with the aim of gaining an advantage over an adversary. It also demonstrates how it is possible to use both (cognitive) Information Warfare and Cyber Warfare methods for operations following the principles of RC. The focus of this discussion is the advantage of combining Information Warfare—as warfare on the cognitive level—with Cyber Warfare, thus manipulating the situational awareness of a modern commander who uses the support of technical solutions in decision-making.

The paper shows that it is possible to use both Information Warfare and Cyber Warfare methods to operate according to the principles of reflexive control. Information Warfare and Cyber Warfare can interact, when RC is applied. One phase of the operation may be mainly characterized as an information operation where cyber operations are employed as supporting functions. The roles may switch in the following phase, during which cyber becomes the main character of the operational phase, in turn supported by informational or psyOPs activities. This kind of interaction is necessary to influence the entirety of adversaries' decision-making processes in today's environment, filling the information space with a variety of information sent through multiple channels. The nature of reporting during the recent conflicts demonstrates this necessity. For example, the conflict in Eastern Ukraine has been not only covered by journalists stationed in the theatre, but also through the vast amount of information available in cyberspace. Investigative journalists today apply tools ranging from tracking soldiers via social media to scrutinizing widely accessible satellite imagery. While reporting certainly plays a role in conflict from the perspective of Information Warfare, it is important to remember that intelligence services also make use of such open source information for their analysis. Therefore, it appears to be of advantage to combine information and/or psychological operations in attempts to create a deception, regardless of whether RC or any other theory or technique has been applied.

The authors have also demonstrated that operations based on RC theory are designed as longer-term operations. They require an intimate understanding of the adversary, its foundations and reactions to various information and stimuli. Likewise, such operations draw advantage from longer engagements with adversaries since those engagements can aim at, step-by-step, preparing adversaries to make a decision predetermined by the initiator of RC. An aggravating factor within these operations is that no exact operation can be used twice, as it would open up the possibility of the adversary's own learning, thus, making the initiator vulnerable to RC. As a result, it is questionable whether RC can be applied in *ad-hoc* activities. Nevertheless, it may be argued that such operations can create decisive outcomes and, thus, may be worth the struggle.

At this point, it is also necessary to remember that RC is but one theory aiming at influencing the adversary. Just as RC may be used in the manner herein demonstrated, an adversary may also be applying either RC or another similar methodology. Therefore, the authors recommend further research into the application of game theory and other methodologies in cyberspace.

The study also shows that there is an advantage to using cognitive operations together with cyber operations. Actions taken in the spheres of cognitive and cyber operations have to be well planned, prepared, and coordinated. Trustworthiness of information is key to their success.

Because this paper is exploratory in nature, the authors strongly suggest further academic research of the individual elements of cooperation in the borderland between cyber and cognitive information.

## References

Bawden D, Holtham C & Courtney N 1995, 'Perspectives on information overload', *Aslib Proc New Inf Perspect*, vol. 51, no. 8, pp. 249-55.

——& Robinson, L 2009, 'The dark side of information: overload, anxiety and other paradoxes and pathologies', *Journal of Information Science*, vol. 35, no. 2, pp. 180-91, doi:10.1177/0165551508095781.

Bryant, DJ & Smith, DG 2013, 'Impact of blue force tracking on combat identification judgments', *Human Factors*, vol. 55, no. 1, pp. 75-89, doi:10.1177/0018720812451595.

Chatham House, *Cyber and space*, viewed 7 February 2016, <http://www.unidir.ch/files/conferences/pdfs/a-review-of-the-chatham-house-space-and-cyber-linkages-project-en-1-983.pdf>.

Hackett, R 2015, 'Here's the scary new target hackers are going after', *Fortune*, viewed 2 February 2016, <http://fortune.com/2015/08/04/globalstar-gps-satellite-network-hackers/>.

Ionov, MD 1995, 'On reflexive control of the enemy in combat' *Military Thought*, English edn, no.1, January, pp. 46-7.

Kantola, H & Hämäläinen, J 2013, 'Modelling cyber warfare as a hierarchic error effect of information', *Proceedings of the 12th European Conference on Information Warfare and Security, ECIW 2013,* Academic Conferences Limited, pp. 322-27.

Kott, A 2015, *War of 2050: a battle for information, communications, and computer security*, U.S. Army Research Laboratory.

Kramer, XH, Kaiser, TB, Schmidt, SE, Davidson, JE & Lefebvre, VA 2003, 'From prediction to reflexive control', *Reflexive Processes and Control*, vol. 2, no. 1, pp. 86-102.

Leonenko, S 1995, 'Refleksivnoe upravlenie protivnikom' ('Reflexive Control of the Enemy'), *Armeyskiy Sbornik (Army Collection),* no 8, p. 28+.

Niu, L., Li, J & Xu D 2000, 'Planning and application of strategies of information operations in high-tech local war', *Zhongguo Junshi Kexue* (*China Military Science*), no.4, pp. 115-22.

Santamarta, R 2014, *A wake-up call for SATCOM security*, Technical White Paper, IOActive, viewed 7 February 2016, <http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_ WhitePaper.pdf>.

Thomas, T 2004, ‘Russian reflexive control, theory and the military’, *Journal of Slavic Military Studies*, vol. 17, pp. 237-56, ISSN: 1351-8046.

——2009, ‘Nation-state cyber strategies: examples from China and Russia’, *Cyberpower and National Security*, eds. FD Kramer, SH Starr & L Wentz, National Defense University and Potomac Books, Dulles, VA, U.S.A., pp. 465-88.

Thurston, M, Stephens, B, Daniels, MR & Steinberger, J 2013, ‘Building a culture of efficiency in blue force tracking technology’, *Defense AT&L*, vol. 42, no. 5, pp. 12-16.

Zetter, K 2015, ‘Researchers hack air-gapped computer with simple cell phone’, *Wired*, viewed 2 February 2016, <http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/>.