Does a weak security discourse provide opportunity for security deviance to flourish?

Michael P. Coole  
*Security Research Institute, Edith Cowan University, m.coole@ecu.edu.au*

Jeff Corkill  
*Security Research Institute, Edith Cowan University, j.corkill@ecu.edu.au*

Follow this and additional works at: [https://ro.ecu.edu.au/asi](https://ro.ecu.edu.au/asi)

Part of the Computer Sciences Commons, and the Social and Behavioral Sciences Commons

**Recommended Citation**  
Coole, M. P., & Corkill, J. (2015). Does a weak security discourse provide opportunity for security deviance to flourish?. DOI: [https://doi.org/10.4225/75/57a83c12d2cf8](https://doi.org/10.4225/75/57a83c12d2cf8)

DOI: 10.4225/75/57a83c12d2cf8  
8th Australian Security and Intelligence Conference, held from the 30 November – 2 December, 2015 (pp. 43-49), Edith Cowan University Joondalup Campus, Perth, Western Australia.  
This Conference Proceeding is posted at Research Online.  
[https://ro.ecu.edu.au/asi/43](https://ro.ecu.edu.au/asi/43)
DOES A WEAK SECURITY DISCOURSE PROVIDE OPPORTUNITY FOR SECURITY DEVIANCE TO FLOURISH?

Michael Coole, Jeff Corkill
School of Computer and Security Science, Security Research Institute, Edith Cowan University, Perth, Australia
m.coole@ecu.edu.au, j.corkill@ecu.edu.au

Abstract
In the years since the tragedy of 9/11 the term “security” has become a much used and abused term. As the war on terrorism has evolved, politicians of all persuasions played the security card to change law and legislation ostensibly to protect the community. Those whom provide the security assume that freedoms lost by the wider community in the name of security are in fact a fair price to pay for that security. In this environment the security discourse is diminished and this provides an opportunity for security deviance to emerge. This research used a selection of publically reported examples of security misconduct to examine and define the construct security deviance. Security deviance being the misuse and abuse of security policy, processes and mechanisms for unauthorised benefit or gratification.

Keywords
Society, security, control, deviance, harm

INTRODUCTION
Security is one of the foundations on which a stable and cohesive society is built, a state often achieved through the provisions of norms and laws. The work of Cotterrell (1984, p. 5) explained law as the practical craft of systematic control of social relations and institutions. It is a discipline concerned with elaboration of the practical art of government; and which, in part, achieves a means of controlling individual actor’s behaviours towards normative behaviours. It was Beccaria (1775, p. 3) who voiced that laws are the conditions under which men, naturally independent united themselves in society. According to Beccaria (1775, p. 6) man, weary of living in a continual state of war, and of enjoying a liberty which became of little value from the uncertainty of its duration, sacrificed one part of it, to enjoy the rest and peace and security. Consequently, the sum of all these portions of liberty of each individual constituted the sovereignty of a nation, and was deposited in the hands of the sovereign as the lawful administrator (p. 6). Such an expression is what supports the notion that a state of no security is not an option. Especially in the view that there are those who seek to undermine such security for their own gains. The very concept of security refers to the application of means of control to remedy the potential and manifested evils of such actors. It is this security that allows citizens to go about their daily lives with freedom and certainty, affording them the ability to make their own choices as to what they do, referred to as freedom of action.

The purpose of this paper is to examine the security discourse for evidence of misuse and abuse of security mechanisms which results in harm to individuals rather than preserving the values they serve to protect. This misuse and abuse is termed security deviance. A range of case studies were selected from the popular media for qualitative analysis.

SECURITY: DEFINITION AND CONTEXT
When scholars, professionals or the lay community define security it is usually done so within an individual or group contextual paradigm. Wolfers (1952) defined security in abstract terms, as the absence of threats to acquired values. Baldwin extended this phraseology to consider the negative effects of natural events. However, Manunta’s (1998) work while accepting that security is value laden, articulated that the very notion of security revolves on three interacting attributes, (a) including a threat, (b) an asset as a referent for values, and (c) a protector, where the value (asset) must be of interest to both the threat and the protector. Nevertheless, Manunta’s model while adequate at a cursory level is lacking when the situation becomes more complex. For instance, ownership of the value is rarely considered and there appears an assumption that protection and ownership have mutually understood perceptions of the threat or equally shared broader values. Furthermore, security is a functional reality that all people and organisations interact with throughout the course of daily activity even though that interaction may be beyond a sensed threshold. Therefore a security dialogue must account for the layman’s contextual concerns to deliver a stable, predictable environment for citizens in their day-to-day lives.
Such discussion provides a useful lens through which to view government and community response to the perceived threat of new terrorism. In this case the threat, terrorism, is recognised by both the government and wider community. The acquired value in this case is a desired way of life. The guardian is the legitimate government through its proxies, its national security community. However the owner of the way of life is not the government, though it does have stake in such, the owner is in fact the national community served. At this point the community as owner of the way of life must determine, what is an acceptable value trade-off between freedom of action and a safe environment? An optimal outcome for the owner is sufficient protection whilst maintaining maximum freedom of action. Whereas the government, as the guardian of that way of life, will seek to influence and persuade the owner of the need for exhaustive security mechanisms in accordance with its perception, and at times, knowledge of the threat. In each case either stakeholder may exploit fear, or the absence of fear, through amplification or attenuation messages, to make the case for their optimal outcome.

However, it is argued that as security control mechanisms expand in the pursuit of security, so do opportunities and instances for their misuse for various gains or gratifications. Such misuse may be state, corporate and private party actions, misusing security’s mechanisms and processes of control for ill gain (deviance). The potential for deviance in the pursuit of security is vast in contemporary society, as security is a multidimensional concept (Brooks, 2009, p. 12). This includes the international and national environmental levels, with reference to the protection of values in the face of malevolent threats (Wolters, 1952; Baldwin, 1997) at a macro level, down to security at the small group-individual level, with references to safety, freedom from fear and retention of belongings (Underwood, 1984; O’Block, Donnemeyer & Doeren, 1991; Craighead, 2003) (stability) as its referent values. Such extensiveness is argued to be represented as two intersecting dimensions where security can be further elaborated to include contextual elements and encompasses military, political, economic, social, environmental or human concerns, achieved through various theories, principles and strategies, and pursued through various means which control or influence potential threat actors’ behaviour to achieve a desired state, that is secure.

SECURITY AS A MECHANISM FOR CONTROL

While an analysis of the literature presents many different contexts and definitions of security, a common theme emerging is that for security to be achieved there must be control. Such a point is expressed in the writings of Cotterrell (1984) and Beccaria (1775) and emphasised within the physical security domain’s language which has adopted the term access control (ASIS, 2009; Norman, 2012). Security as a social construct is argued to be a lulling term for control through the use of what Weiten (2002, p. 258) refers to as ‘semantic slanting’. This refers to the use of language to deliberately choose words that create specific emotional meanings. In security’s case this is to imply a provision rather than impose control or power over others. This includes a means of direct control, or power to influence to achieve indirect control. For example, Cohen (1966, p. 48) stated:

“A control conception of human motivation is built around two sets of variables. The impulse side: a hostile, destructive, aggressive, acquisitive, or otherwise "antisocial” impulse. And a control side: something inside the actor or in the situation of action that denies or forbids the expression of the impulse. The outcome depends on the relative strength of these two contenders: if the impulse is stronger the outcome is deviance; if the controls are stronger, the outcome is the inhibition of deviance”.

Such a point is evident when analysing the themes emerging across the various security contexts in relation to the various definitions of control. Definitions which include (a) to command or rule, (b) to check, limit or restrain, (c) to regulate or operate, (d) to regulate, (e) and to examine (Hanks, Makins, & Adams, ND). Such themes of control are embedded in the various discourses on security. For example, Ullman (1983) argues that for society to work there must be control, both externally and militarily (traditional security), and internally through other mechanisms (non-traditional security). For instance, drawing on Hobbes, Ullman (1983, p. 130) argued that regardless of whether threats to security stem from within or externally of one’s own nation, a victim is still a victim and so citizens within a state seek protection against both types of threats, that is foreign and domestic.

Ullman’s work draws on Hobbes to emphasise that a lack of control in one environment, regardless of the controls in others would still result in peril, introducing security as an absolute value, where the state directs how much control it requires to provide a level of security (Ullman, 1983, p. 130). Consequently, to achieve security there must be value trade-offs, with higher values taking precedence over lower values, where higher values such as security includes mechanisms of control versus freedom of action. Such mechanisms arguably include policies, laws, physical, technical and operational means as an integrated system of societal control.
A critical analysis of the broader security discourse supports the contention that security is pursued through a defined level of control within a context, be it globally, nationally, at a State level, organisational level or domestic—individual level. Such control is achieved collectively, politically and systematically in a defined manner to achieve stability and predictability. That is, functionally security is the application of sufficient control mechanisms to ensure a safe environment of which enables a nation, organisation, or individual the freedom of action to engage in an activity in a specific context. Consistent with the very premises of Beccaria (1775) a control thesis of security arguably means a reduction in freedoms, choices and privacy, reduced through mechanisms which aim to provide a, macro-to-micro safe, secure environment.

Furthermore, consistent with the liberties versus security dialogue, Ullman (1983, p. 130) acknowledged that total control is an extreme value (prime), at odds with the desires of the wider community (marginal value) whom aim to balance security needs against other, perhaps core values (Baldwin, 1997) including economic prosperity, freedom and privacy. Consequently, citizens also seek security against the State, or more specifically against excessive controls potentially, or enacted by the state to achieve its preferred level of security. Thus, a discussion of security encompasses a discussion concerning values in terms of levels of control, real and perceived across all strata of society. Newman (2010) considered security to be about the pursuit of policy, which if correct, is a policy to gain and maintain a level of control accordant with values within an environment, where security resources are steered to achieve such control.

SECURITY DEVIANCE

The notion of security deviance is grounded in the view that wherever there is control or power to influence in the pursuit of control, there is the potential for, and incidence of deviance, which in this discourse is the misuse of security policy, processes and mechanisms for unauthorised benefit or gratification. As Taylor, Walton and Young (1973, p. 140) noted, attempts to deter, punish and prevent deviation can actually create deviation itself. It is in this framing that the concept of security deviance can be understood. Deviance is a concept readily identified throughout all strata of society (Box, 1971; A. K. Cohen, 1966; Erikson, 1961; Garland, 2001; Innes, 2003). The notion of security deviance can be framed by the works of Cohen, who explains that all societies, subgroups and institutions have rules which when violated draws emotive responses including disapproval, anger and indignation. Cohen (1966, p. 3) stated that if human beings are to do business together there must be rules, and people must be able to assume that, by and large, these rules will be observed, while also acknowledging that where there are rules there is accompanying deviance (1966). Extending this view, Box (1971, p.9) and Taylor, Walton and Young (1973, p. 140) highlight that deviance is not restricted to acts which break formal rules, emphasising it also results from the social reaction to other acts which label the acts deviant in hindsight. Consequently, the very mechanisms of control to achieve a state of security can, and at times will be exploited by the willing, and such exploitation is a form of deviance.

According to Cohen (1966, p. 4) deviance can impact society in three salient ways: it can be analogous to the loss or defect of a critical part in a delicately coordinated mechanism; or it can undermine an organisation by destroying people’s willingness to play their parts, reducing their contribution to the ongoing activity; and it can destroy trust, destroying confidence that individuals will play by the rules. Consequently, if we accept the values discourse of security and acknowledge that security is pursued through mechanisms of control, then it must also be acknowledged that abuses from such measures is a human reality.

Fear and the amplification or attenuation of fear messages has contributed to the all-pervasive nature of security in the lives of all people. Lianos (Lianos, 2000, 2003) introduces a concept of institutional control as a natural evolution from social control and one in which fear, suspicion and vulnerability all contribute to a greater desire for security. Whilst Lianos argues that to some extent the construct of ‘dangerization’ means an end to deviance in fact the authors would argue that the ‘safety paradox’ to which Lianos refers actually adds weight to the argument that security control mechanisms may be exploited in a deviant manner. “In terms of social organization, this can be represented by a vicious circle: institutional activity → control → predictability → safety/certainty → vulnerability → dangerization → new claim for control → new institutional activity...and so on” (Lianos, 2000, p. 275).

The control expressed by either a nation state or institution is represented in the language of the security it provides towards managing those threats which pose a risk at either a global, national, State, organisational, or domestic–individual levels. Such an expression raises the question, how is the breadth of such control represented in any given society, and where are the opportunities for, or incidences of security deviance accordingly? The breadth and multidiscipline nature of the security domain suggests control is persuasive across all strata of society and therefore opportunities for deviance within the mechanisms of control are as broad as
the security domain itself. It is argued that due to the embeddedness of security in contemporary society, such deviance can undermine the very fabric of a social system and is therefore a serious issue to be addressed.

**REVEALING DEVIANCE ACROSS THE STRATUM OF SECURITY**

Security deviance can be manifested by a nation state or its agencies, against its people, by government officials, misusing the pursuit of security for other gains, by corporations, and by individual security actors. For instance, the social contract refers to the means where citizens and the state agree on the provisions of protection in exchange for traded freedoms, this exists on a continuum in which control waxes and wanes according to the trade-off between security and liberty. A theory of social control according to Johnson (1995, p. 258) seeks to explain the origins and binding force of mutual obligations and rights in society, protection for the submission of authority.

Deviance is considered as any behaviour or appearance which violates societal norms (Johnson, 1995, p. 78), where security deviance is an extension of this articulation to contextualise deviance stemming from the misuse of security. The concept of deviance is a significant concern within the sociological literature with much of the focus steered towards the unintended consequence of police control (Abercrombie, Hill, & Turner, 1986, p. 67). These authors point out the sociological approach in a broader sense sees deviance as a socially prescribed departure from normality where many different, even non legal forms of deviance may be condemned taking a more heterogeneous category of behaviours as its lens of enquiry towards deviance within any given society. Therefore, security deviance considers deviance from a broader perspective, focusing on the security domain as its lens of purview. The five cases below provide brief examples of how security deviance may manifest its self across the various stratums of the security domain.

For example, in the United States the National Security Agency (NSA) has admitted various wilful violations of “agency protocols”, when officers used surveillance tools to spy on romantic interests, labelled LOVEINT. Further reports note NSA officers, in their pursuit of security, intentionally breaking the law around 3,000 times in a 12 month period, with NSA lawyers arguing that “sometimes agents had to break the law due to technical limitations”. A 2012 NSA audit highlighted that some agents abused their power to intentionally spy on Americans (Jason, 2013; Peterson, 2013).

In Australia customs border security staff at Sydney airport were prosecuted for using their security roles as a means of importing drugs for distribution. These border security staff were exploiting the systems of security for their own financial gains, which included practices such as manipulating staff rosters to facilitate their illegal operations. Both are examples of how security personnel in national agencies have exploited the very mechanisms of security control for deviant gains. However, deviance has also been well reported in the community security domain, with specific emphasis on CCTV misuse for personal gratification (McKenzie & Baker, 2012).

In Australia A Current Affair television program reported on security guards at Westfield Shopping centre in Sydney stalking women via CCTV, then tagging them with labels, storing and later sharing the footage in what was described as a “Sleaze file”. The report purported that the misuse of security cameras, particularly against women had been happening for years and is still occurring, including “zooming in on women sitting down wearing short skirts”. Television Reporter Marin King is quoted in press as saying, “It becomes an absolute outrage when security guards who are supposed to be protecting us, are instead prying on innocent women” (Cummins, 2015; Doctorow, 2015; King, 2015).

The misuse of CCTV footage has also been publically reported in the United Kingdom (UK), where public officers have been found to be exploiting footage for personal gain. For example, public officers in Northumbria were disciplined when it was found that they took close-up pictures from CCTV footage that captured 1500 naked volunteers who participated in a photo shoot for artists Spencer Tunick in Newcastle and Gateshead. The officers offered close-up photographs of some of the nude volunteers for sale (Ward, 2006). Another such UK incident involved council workers misusing a public street surveillance camera (CCTV), repositioning the camera to spy on a woman in her apartment. The public officers filmed the women undressing, bathing and going to the toilet, and allegedly showed the footage on a large screen in the Sefton Council control room in 2004 (“Peeping tom CCTV workers jailed,” 2006).

Finally, in Australian politics the period of the Abbott Prime Ministership saw extensive amplification of national security concerns and calls to the danger of terrorism as a means to create fear or concern in the wider community that enabled the government of the time considerable freedom to impose restrictions on liberties that would otherwise be resisted. This was particularly notable on the issues of meta-data retention and terrorism (Gittins, 2015; Keane, 2015; Matthewson, 2015; Tingle, 2015; Wroe & Kenny, 2015).
Do the presented cases support the notion of security deviance? According to Abercrombie, Hill and Turner (1986, p. 68) deviance studies have embraced a great diversity of behaviours including drug abuse to football hooliganism where it is argued that extending the concept into the security domain is a natural, and given the embedded nature of security in modern society, logical extension of previous works. As Anthony and Cunneen (2008, p. 148) explain, directing a lens of purview towards the systematic abrogation of people’s rights is not new for critical criminologists, especially in the manifestation of social injury through the violation of legal rules or cultural, moral norms. However, this discourse is often directed to deviance of the state. Yet security deviance can be those actions against the state, or actions committed by the state or its agents or private parties in the pursuit of reward.

The notion of security deviance is framed within a human rights approach to security where the ever complicated trade-offs between societal safeties and well-being as afforded by control versus reduced freedoms of choices or actions must be considered against conceptions of social injury (Anthony & Cunneen, 2008) in terms of harms inflicted against people in its pursuit. It is important to note that in terms of exploiting the mechanisms of control implemented to provide a secure environment, collectively a coalition, state, organisation, group or individual can engage in deviance within the context of a social harm model. However, security deviance must not be limited to purely social harms, it must be considered holistically within the two intersecting dimensions of security where consistent with Anthony and Cunneen (2008) it must also embody macro deviance which results in serious human rights abuses down to micro-level-deviance such as fraudulent materials gains; that is a macro-meso-micro model of deviance. Again, such deviance can be manifested by a coalition, state, organisation, group or individual, resulting due to the pursuit of, instrumental gains, the maintenance of influence or control, justified through rationalizations. Security deviance as a concept relates to Cohen’s (1993) expressed concerns where the very agents responsible for providing societal security are actually responsible for various acts of deviance facilitated by exploiting accepted mechanisms of control.

**CONCLUSION**

The very concept of security inclusively allows individuals, organisations, nations and humanity freedom to act in appropriate ways within a specific context at a specific time according to norms. However in order to exercise that freedom control mechanisms must and will be applied through all strata of society from the international arena through to the individual domain. Such security control mechanisms may be explicit or they may be implicit, irrespectively they are contextually specific and may be exploited for deviant gains. The depth and breadth of the security domain means that opportunities for deviance stemming from the misuse of security are vast; consequently, such opportunities need to be clearly identified. Security control mechanisms may include, legislation and law, rules and regulation, and policy where security deviance may arguably occur at that point where such mechanisms extend beyond sufficient control. Security deviance must be considered as a two-sided theory within the variability of both impulse and control as it represents a threat to effective and necessary stability mechanisms through its potentially corrosive impact on community trust. Whilst this research is still in its early stages it is the authors view that carefully mapping the security domain with an aim to identify and catalogue forms of security deviance will enable a better balance to be achieved in the trade-off between liberty and security.
REFERENCES


