Chapter 14
Case: Dronebuster; Handling Non-compliance to ITAR

Wim Nieboer and Dik van Manen

Contents

Abstract This chapter analyses the unauthorized transfer of a Dronebuster for testing in a fictitious European NATO member state (EUMS). As the Dronebuster had been purchased in the US, it remained subject to US export control regulations, and, prior authorization was warranted. As there had been no requests for prior authorization, this transfer is considered non-compliant behaviour. Using the Problem-Oriented Policing framework, we investigate the underlying causes and conditions. We argue that a coordinated operation of a mix of hard- and soft controls is the optimal response to prevent such behaviour.

Keywords Arms export control · awareness · Dronebuster · (non-)compliance · ITAR · NATO

W. Nieboer (✉)
NSPA, Rue de Gare 11, L-8302 Capellen, Luxembourg
e-mail: NELO@NSPA.NATO.INT

D. van Manen
Export Control Compliance Team CLAS, PO Box 90004, 3509 AA Utrecht, The Netherlands
e-mail: d.v.manen@mindef.nl

© The Author(s) 2022

R. Beeres et al. (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2021*, NL ARMS,
https://doi.org/10.1007/978-94-6265-471-6_14

14.1 Introduction

This chapter describes and analyses a situation of non-compliance in relation to the US export control regulations, more specific the International Arms Trade Regulations (ITAR). We consider an unauthorized transfer of a so-called Dronebuster from the Army to a National Research Institution (NRI) for research purposes in a fictitious, non-existent European NATO member state (hereafter named EUMS).

Some years ago, the Ministry of Defence (MoD) of the EUMS purchased a number of Dronebusters to serve in missions against drone threats. In the slipstream of an investigation on drone threats and a range of counter measures by Dronebusters taking place in the vicinity of EUMS airports, it was deemed necessary to investigate the impact of Dronebusters on other electrical and electro-magnetic systems present. Without much ado, the Army proceeded to submit one Dronebuster for closer testing by the NRI, specifically with regard to the Dronebuster's electro-magnetic impact on other systems.

By the time the MoD's Export Control Compliance Team (ECCT) became aware of the Dronebuster's transfer to NRI, the item had already been tested and returned to the Army. However, as the Dronebuster, an export controlled item under the International Traffic in Arms Regulations (ITAR) had been purchased in the US by the MoD's Direct Commercial Sales (DCS), handing it over to NRI—outside the MoD—would have required prior authorization by the US. As it turned out, the Army was neither aware of the Dronebuster being an export-controlled item nor that prior authorization for the transfer should have been mandated.

Based on the Problem-Oriented Policing (POP) framework, our case-study serves as an investigation into the underlying causes and conditions of this unauthorized transfer.[1] We ask what causes and conditions have resulted in the unauthorized transfer of the Dronebuster. Section 14.2 introduces non-compliant behaviour in this (hypothetical) case study. Section 14.3 analyses the causes at the macro-, meso- and micro-levels. Derived from information gathered in the third section, in Sect. 14.4 we develop an appropriate response. In the final section, Sect. 14.5, we discuss our findings.

14.2 Scanning

A Dronebuster is an efficient tool for preventing drones to approach secured areas or own troops. A Dronebuster operator can jam the drone command link causing it to hover or return home. Also, the signal can be jammed to the extent a drone will crash or land. The operator only needs to pull and hold the trigger of the Dronebuster. Dronebuster Block 3 is an export controlled item under US export control regulations, specifically, ITAR. Furthermore, Dronebusters have been classified as Significant Military Equipment.

[1] Braga 2008.

EUMS MoD acquired Dronebusters to serve in missions, either domestic or abroad, against drone threats. When it became necessary to investigate the impact of Dronebusters on other electrical and electro-magnetic systems at airports, the Army offered one Dronebuster to NRI for testing. Additionally, NRI requested to be allowed to open the systems for further investigations. However, this request was denied by the MoD, on the grounds that, re-transfer of a Dronebuster, its data, software etc. to parties outside the EUMS MoD is not allowed without prior authorization by the US government. At the time the Army's Export Control officer was notified of the transfer to NRI the item had already been tested and returned.

Previous investigations into this case have clarified that officers and staff involved in this Dronebuster transfer to NRI were unaware of the requested prior authorization, both in case of transferring as well as testing export controlled items. The main issue here appears a lack of awareness among all involved personnel.

This raises several questions for further analysis. First, as export control was already relatively well known within the EUMS MoD why were these officers and staff not informed on the export control implications of a Dronebuster transfer to NRI? Second, information on the export control classification is available and visible whenever employees attempt to transfer export control items outside the MoD. Why did the personnel involved fail to react to this information? Why were they not aware of the implications of the export control references? Why did the internal control system not operate as expected?

14.3 Analysis

14.3.1 Macro-level: Export Control Laws and Regulations for the MoD

Export control laws and regulations; international as well as national have been in place for a substantial period of time, starting with treaties on weapons of mass destruction after World War II. In modern warfare, export control frameworks have become more comprehensive and influential. For many years the EUMS MoD did not fully appreciate their relevance for daily business and operations, although a fair number of EUMS' weapon systems and equipment were acquired in the United States, and, consequentially, remained under US export control regulations.

In 2011, both an investigation into the relevance of export control regulations regarding the EUMS MoD, as well as the (non-)compliance situation, at the time, made clear export control still was not very high on the agenda. This all changed, as it transpired that some serious violations of export control regulations had taken place within the EUMS Airforce. Voluntary disclosures were brought to the attention of the US government, thereby turning into a sensitive political issue for the EUMS government and parliament. As at the macro-level the political and regulatory consequences became increasingly clear and explicit, at the meso-level, the

organizational level of the MoD, actions were required. As a result, commands and instructions started cascading down the Operational Commands (Navy, Army, Air Force) requesting commanders to implement export control regulations and to install and execute internal compliance programs.

14.3.2 Meso-level: The EUMS Army

From 2014, the Army started implementing export control regulations. At the time, the Army's slogan was they were using 'a raincoat and a sharp pocket knife' instead of any technologically advanced equipment. At all Army levels, knowledge on Export Control was limited, and personnel largely remained unaware of any legal, moral or ethical issues involved.

In 2016, it became clear that something had to be done about this awareness and knowledge gap as the Army increasingly acquired advanced equipment and specific technology from the US and therefore subject to ITAR. The Commander of the Army started their internal compliance program in 2016. At unit levels, serious handling of export control regulations did start from 2016 by describing an internal compliance program and by introducing a dedicated organizational unit within the organization. By the end of 2018, this organizational unit has turned into a standing unit (i.e., the Export Control Compliance Team).

Amongst others, internal compliance programs (ICPs) are to raise organizational awareness on the relevance and importance of export control laws and regulations. And this is where the Dronebuster case went askew, for, as it turned out, involved personnel were completely unaware of export control implications of their actions. Looking back, it seems obvious that, when starting with the construction and implementation of an ICP, awareness will not be raised throughout the organization immediately.

However, four years later, in the EUMS Army, the Export Control Compliance Team is still on the road, regularly spreading the export control news. A lot has been invested in these roadshows on behalf of commanding officers and relevant staff in security and logistics, as well as the organization of training and publishing on intranet. Education and training is one of the Key Performance Drivers for a Defence Organization. Export Control was a relatively new feature within the EUMS MoD, and lacking appropriate training/education has led -and sometimes still does- to non-compliant actions. Familiarity with Export Control regulations increases compliance (e.g., by training and information sessions) and will contribute in Export Control compliance in general.[2]

Communication and training have undoubtedly contributed to an increased awareness at the organizational level. However, as the Army is a large, multi-layered organization, awareness levels are expected to vary across the organization and its various units. As it is possible, bureaucratic rules and regulations can facilitate non-compliant

[2] Gelderman et al. 2006.

activities, transparency and accountability at all organizational levels should be aimed for. Obviously, the MoD's export control organization is still 'under construction', progressing towards maturity.

14.3.3 Micro-level: Awareness of Individuals

At the micro-level, the level of the individual employee (commander, staff, soldier), actions taken at the macro- and meso-level appear to induce increasing levels of awareness. Personnel directly involved in security and logistics, in general, are both knowledgeable when it comes to export control as well as experienced in using ICT systems and in cooperation with export control support teams. Nevertheless, as the non-compliant behaviour regarding the Dronebuster has made clear, there is still work to be done in this respect.

At the micro-level, one important characteristic of the EUMS MoD is vital when planning to increase employee awareness. This regards the fact that military staff rotates every three years, and sometimes even faster. Consequentially, raising knowledge and awareness knowledge and awareness within the various units of the organization has to be undertaken as a continuous endeavour, deserving constant attention.

It is clear that introducing measures (e.g., ICP) at an organizational (meso-)level does not automatically imply compliance at a (micro-)individual level. Because all three organizational levels are intertwined, a problem and a solution at one level will always need additional analyses at the other levels. Therefore, serious investments in staff and personnel will be required, also considering other specific characteristics of military personnel (e.g., can-do mentality).

In the Dronebuster case, export control regulations were not lived up to because employees were unaware of export control implications of their actions. On top of this, however, it appeared the implications of this neglect were underestimated and even disregarded. One of the EUMS Army's paramount guidelines is the mission must be fulfilled, no matter what. 'Make it happen, no matter what' may be considered an Army maxim professing a positive organizational culture, although it comes with a serious downside, regarding its potential to instigate non-compliant behaviour in the workspace.[3] At the micro-level, such maxims can result in employees believing that, in order to fulfil the mission, laws and regulations may be avoided or even circumvented. Although such behaviour may be considered adequate during missions and other operational situations, in peace situations, concerning export control regulations, this will thwart and even obstruct the effectiveness of new rules or reforms.[4]

As it turned out, employees rationalized their unawareness and breaking of relevant export control regulations by pointing at the organization, that did not 'educate'

[3] Griffin 2013.

[4] Interligi 2010.

them sufficiently in this respect. The fact that the system of internal control was not fully functional may have added to this feeling. Furthermore, Army employees, mandated to execute actions within their own work field in combination with not fully operational internal controls (e.g., an ICT system not blocking transactions when proper authorizations are lacking) opens the possibility to violate, either knowingly or unknowingly, export control regulations. A process which excludes *all* possible mistakes or deviance seems unfeasible (opportunities continue to exist for those who want to be deviant/non-compliant). According to cognitive dissonance theory forced Export Control compliance can culminate into cognitive dissonance or non-compliant behaviour.[5] Therefore, constant control and monitoring remain necessary.[6]

14.4 Response

According to the definition of the Association of Certified Fraud Examiners,[7] the EUMS Dronebuster case can be defined in terms of fraudulent reporting or fraud on behalf of the organization, aiming to make the organization look better than it is. This sounds somewhat harsh, and one may argue whether this constitutes actual 'fraud'. In almost all Defence cases bearing resemblance to this one, there is no motive for personal gain (nothing is taken away), instead, the main driver for non-compliant behaviour appears to be to create an image of an organization functioning properly. Employees, not considering the appropriate regulation, appear to want to fix an issue. Thus, instead of fraud, we refer to this kind of behaviour as non-compliant or deviant behaviour.

Building on Braga's[8] problem-oriented policing and crime prevention, and to induce potential novel ways for proper behaviour, we have applied a model presented by Cornish and Clarke.[9] The authors use the idea of situational crime prevention as a starting point, and, from here, have developed a related list of techniques and specific programs. To us, this model has been useful because it urged us to think more in-depth instead of aiming for short term success.

In a reflection on Cornish and Clarke, we suggest the following responses. First, introduce controls to complicate deviant behaviour (i.e., clear procedures; working internal controls in IT systems; no manoeuvre or escape possibilities; and access authorizations in accordance with one's role). Second, increase the risk of exposure of deviant behaviour (i.e., extend action responsibility from one officer to two or more officers; separate duties, roles, and responsibilities; four eyes principle; peer reviews and audits focussed on export control). Third, reduce rewards for deviant

[5] Festinger 1962.
[6] Huberts et al. 2008.
[7] Murdock 2019.
[8] Braga 2008.
[9] Clarke 1995.

behaviour (i.e., clearly communicate rewards for correct export compliant behaviour as well as disciplinary actions following from non-compliance).

Fourth, clarify stressful situations and procedures. Often, employees experience a sense of operational urgency when handling items with export control regulations. The lack of an optimized controlled process induces uncertainty and anxiety, causing them stress. Clear procedures and training as well as adequate support by an export control compliance team, would take away stress and frustrations. Internal controls by ICT systems would support this. Fifth, prevent any excuses for deviant behaviour. Neither procedures nor the system should allow for deviant behaviour. So the parts/items should be identified, and applicable sets of regulations should be implemented in the systems. An Internal Control System should be implemented and periodically audited. HRM involvement could improve recruitment, initial screening/selections and background screening, which in their turn may improve the quality of new personnel intakes. Training allows employees to acquire new skills, improve on existing ones, perform better, increase productivity and to become better leaders. As an organization is made up of the sum total of what its employees achieve individually, organizations should do everything in their power to ensure that employees perform at their peak.

14.5 Assessment

In this chapter we have used Braga's POP-guide as a lens to look at an export control problem. We have analysed the occurrence of non-compliant behaviour in a fictitious case, entailing an unauthorized transfer of a Dronebuster from the Army to a National Research Institution (NRI) for research purposes within a fictitious European NATO member state, EUMS. Based on our analysis, we have suggested a number of responses. In sum, these responses add up to a coordinated mix of hard- and soft controls. As a short-term response, soft controls (e.g., training, education, development and communication) have to be priorities. In the long run the internal control system (including a proper audit plan) should be in place and development, training and communication on export control is to be secured in the organization. The internal control system should minimize the possibility of deviant actions (e.g., registration and obligated process flows with blockages).

During the analysis of the EUMS Dronebuster case, it was interesting to investigate both actual deviant behaviour as well as possible solutions. A question that remains to be answered is why the NRI did not react on reception of the items. For NRI also should have been aware of export control implications as well as of the fact there was no US authorization of the item received for investigation. We would like to recommend this question for further study.

References

Braga AA (2008) Problem-Oriented Policing and Crime Prevention, 2nd edn. Willow Tree Press, New York
Clarke RV (1995) Situational crime prevention. Crime and Justice 19:91–150
Festinger L (1962) Cognitive dissonance. Scientific American 207:93–06
Gelderman CJ, Paul WT, Brugman MJ (2006) Public procurement and EU tendering directives–explaining non-compliance. International Journal of Public Sector Management 19:702-714
Griffin RW (2013) Organizational Behavior. Oxford University Press, Oxford
Huberts LW, Maesschalck J, Jurkiewicz CL (eds) (2008) Ethics and integrity of governance: Perspectives across frontiers. Edward Elgar Publishing Limited, Cheltenham
Interligi L (2010) Compliance culture: A conceptual framework. Journal of Management and Organization 16:235–249
Murdock H (2019) Auditor Essentials: 100 Concepts, Tips, Tools, and Techniques for Success. CRC Press, New York

Wim Nieboer is a major with the Netherlands Army with a technical background. Currently is he employed as the Netherlands Liaison Officer with the NATO Support and procurement agency in Luxemburg. His research interests include ethics and compliance of export controls and related EU NATO possibilities, and impossibilities.

Dik van Manen is head of the Export Control Compliance Team (ECCT) with the Netherlands Army.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.