9

A Two-Level Account of Executive Authority

MICHAEL SKERKER

National security programs create challenges for advocates of popular sovereignty—the idea that "we the people" broadly, should govern ourselves. In a democracy, the people elect officials to govern them and hold these officials accountable, in theory, by monitoring their actions and subjecting the officials to regular re-election. Thus, transparency appears to be a precondition for popular sovereignty. Alex Guerraro lays out the challenges for this kind of accountability in his chapter in this volume, particularly with respect to national security issues. Few citizens know what their officials are doing; the issues at hand are exceedingly complicated, and in the national security realm, certain deliberations, decisions, and actions often have to be kept secret to preserve their efficacy. Thus, a paradox: in a system where the people are sovereign, people elect officials in part, to keep them safe; national security actions may require secrecy, but secrecy undercuts the legitimacy of government action in a system where the people are sovereign. The purpose of this chapter is to determine whether inhabitants of a liberal state—a type of state tracing the legitimacy of its coercive actions to the consent of the governed—also need to know the internal protocols and legal findings of the government agencies ostensibly serving them. To put this question another way, what, if anything, may government agencies in liberal states keep secret?

This chapter will proceed in four sections. It is first necessary, in Section I, to articulate a moral foundation for security operations—law enforcement, military, and intelligence operations—conducted by a state domestically and internationally. The argument for grouping these types of operations together is that they are all oriented to maintaining a secure and peaceful domestic society. Moreover, liberal states divvy up security responsibilities among different agencies in various ways, so it would not serve the purpose of this chapter to restrict the conversation to one agency or activity. A moral foundation will express the rationale for security services such as law enforcement, military, and intelligence agencies to

Sovereignty and the New Executive Authority. Claire Finkelstein and Michael Skerker.

engage in operations. This foundation will also provide a possible justification for maintaining secrecy if secrecy is necessary for the success of security operations. Section II will ask if public scrutiny of security services is necessary. Section III will ask if laypersons are competent to scrutinize the operations of security services. After it is determined that public scrutiny is both appropriate and possible, Section IV will consider whether and how security services can effectively deliver security while also making internal protocols, legal rulings, and operations public. I conclude that many types of security operations can survive public disclosure at a certain level of generality. A relatively small number of morally permissible operations must be kept secret when their disclosure would directly or indirectly endanger security personnel or the success of operations.

I. MORAL FOUNDATIONS FOR SECURITY OPERATIONS

A. Institutions, Collective Responsibilities, and Professional Duties

The purpose of this section is to develop a moral foundation for a state's security operations. I will initially rely on technical work done by Seumas Miller to explain the moral foundations of institutions.

Human beings have positive and negative claim-rights by virtue of their natural properties. These rights impose reciprocal positive and negative duties on all others. One person can meet her positive duties toward another by delivering morally required goods and services in circumstances when positive rights are apt and the duty-bearer is in the morally relevant position to deliver those goods and services. For example, many argue that all humans have a positive claim-right to the basic goods for a decent life such as food, shelter, and medical care. If this is true, it follows that a very poor person without the means of providing for herself (perhaps because of disability or scarcity in the local environment) may demand assistance from a well-off person with the power to help her. While anyone *can* demand anything of anyone, the structure of rights suggests that the well-off person is duty-bound to positively respond to the poor person's demand. All humans also have negative claim-rights against being murdered, assaulted, robbed, raped, deceived, and so on, which all others (not merely those in the patient's proximity or those with certain means) can meet by refraining from such rights violations and by protecting her from them.

Individuals also have joint moral rights insofar as they are members of certain groups. These are rights that attach to individuals but only as group members: for example, a right of national determination or a right to secede. They are based on properties individuals have as individuals, such as a right to direct one's own life, as well as on properties they have as group members.[1] A joint moral right of special relevance to this chapter is the right to security, by which I mean a right to live in an environment that is free of rights violations to a degree that people are not unduly inhibited from pursuing different personal and joint projects. This

1. Seumas Miller, *The Moral Foundations of Social Institutions* (Cambridge: Cambridge University Press, 2010), 68.

right will be unfulfilled in most complex societies absent institutions to deter, investigate, and punish rights violations as well as a culture (partly shaped by the relevant institutions) where most people are disinclined to intentionally commit rights violations.

If a person is well-off and can buy the necessities of life for himself, his positive right to these goods does not impose duties on others. The fact that everyone, well-off and not, needs these goods creates a collective moral responsibility to create them.[2] Thus, if for example, a group of shipwreck survivors find themselves on a deserted island, it is intelligible for them to say "Somebody *should* go gather fruit," where the "should" has normative, and not just instrumental weight. The person engaged in these activities, or in producing such goods in a complex society, has a certain moral privilege to her actions, to be further refined below.

The aggregation of individual rights, joint moral rights, and aggregated human needs create collective moral responsibilities to protect and address those rights and fulfill those needs. Collective moral responsibilities are moral responsibilities of groups to attend to these rights and needs because only groups can effectively meet them. Groups are not supra-individuals with special group-sized responsibilities. Collective responsibilities attach to individuals but only if they are members of certain types of groups.

Typically, these collective moral responsibilities are acquitted by creating and supporting institutions to address the relevant rights, such as schools, hospitals, businesses, churches, and militaries.[3] Governments are meta-institutions tasked with coordinating the activities of institutions. These institutions are essentially teleological, set up to foster, create, and protect the collective moral goods (e.g., health, education, security) that protect rights and fulfill morally important needs.[4]

The collective moral responsibility of society is largely, though not completely, transferred to the professionals who work in morally vital institutions. For their part, laypersons should support the work of these institutions (subject to certain limitations, below) by cooperating with institutional actors, obeying relevant laws, supporting the institutions though tax payment or charity, and refraining from attempts to undermine them. They might also be morally required to directly assist institutional actors in cases when they cannot cope with exigent circumstances, such as helping clean out debris after a natural disaster.

The end of these institutions are collective goods so professionals have a joint moral duty to comply with their professional imperatives (a joint moral duty is a moral duty to do something that can only be done in a group).[5] Thus professional imperatives are not simply like the obligations of a member of a club, instrumental to the club's end, but moral duties, with the weight to compete with other moral

2. Miller, 68.

3. Miller, 57, 77, 80. See also Paul Camenisch, *Grounding Professional Ethics in a Pluralistic Society* (New York: Haven, 1983), 52–55.

4. Camenish, 54–55.

5. Miller, 80.

duties, since they meet others' positive rights, protect negative rights, and produce the goods to meet morally important needs.

A professional duty to meet the collective moral right of security is too vague to be action-guiding for professionals such as police and service personnel. At first blush, we can see that many steps to deliver security could be unacceptable to the community supposedly benefited by the state agents, for reasons ranging from brutality to ineffectiveness. I propose we take advantage of the criterion of universalizability inherent in most schemes of rights and duties to further delineate relevant professional duties. Since a key component of deontological morality, on most construals, is the equality of human persons, one way of working out the scope of attendant schemes of rights and duties is through universalization tests. In order to identify rights and their scope of legitimate exercise, philosophers imagine everyone in the world who is capable of bearing rights as having the putative right under discussion and potentially planning to act or actually acting on the right to the proposed degree. Plans or actions that cannot be logically or practically universalized, or rules for actions or permissions to act that cannot win actual or theoretical consent by those potentially affected by the action, are morally impermissible. Non-universalizable rights-candidates fail and thus lack correlative duties.

I propose that the contours of security professionals' duties to contribute to security be specified by imagining the professional behavior winning the universal, hypothetical consent of all the parties affected by the agents' action. In non-philosophical settings, people invoke hypothetical consent when they consider what an acquaintance or a stranger would find consent-worthy when the agent is unable to communicate with the other party. Considerations of what an acquaintance would consent to might be based on particular knowledge of the person's preferences. Considerations of the same question in relation to a stranger must turn on assumptions about what any person would have rational grounds to find worthy of consent. We assume someone experiencing a medical emergency would want to be given first aid, we assume someone who has passed out from hunger would want to be fed intravenously, we assume someone being attacked would want to be defended, and so on. This strategy does not give the agent a wide range of action-guiding directives but will be limited to actions geared toward protecting generic human interests or moral qualities. The agent has rational grounds to think that anyone would consent to proportionate actions taken to save the person's life, limb, and property and to protect her rights because every person has rational grounds to demand and seek the preservation of these interests and rights in her own case. An actual person might not want to live, be fed, or have anyone harmed on her account but has rational grounds to demand satisfaction of ofher rights. She cannot blame a stranger for assuming her desire for rights protection absent some express sign to the contrary.

Philosophical discussions of hypothetical consent sometimes idealize the consenters and/or the context for consent in order to screen out biases, idiosyncrasies, and immoral views actual people may have, and nonideal factors characterizing actual debate on moral issues such as ignorance, limited time, intimidation, and other non-rational group dynamics. These thought experiments

are conducted by some in an effort to identify a fundamental framework for all of interpersonal morality or for identifying just political institutions. My use of hypothetical consent will be less ambitious than both of these projects, using it instead to identify the contours of extant professional duties.[6] As argued above, I agree with Miller that the properly constituted professional duties of morally vital institutions are moral duties. Hypothetical consent is one way—not necessarily the only way—of working out the proper constitution of professional duties. To be clear, I am not using hypothetical consent to ground professional norms, but rather, as a heuristic to work out the unvarying norms entailed by professional duty and the derived professional tactics, that vary with context as applications of the norms.[7] Professional morality is ultimately grounded in the collective moral responsibility to protect people's joint moral rights, aggregated individual rights, and aggregated needs.

I will refer to the hypothetical consent of all affected by potential state actions below without specifying which social contract school's notion of consent is being invoked: the consent of idealized consenters operating according to ideal communication rules, of actual people following ideal communication rules, or of actual people unconstrained by ideal communication rules.[8] It is appropriate to

6. I am sympathetic to both projects but lack the space here to work out a full-blown contractualist theory or refine the political contractualist model I developed in chapter 2 of *An Ethics of Interrogation*.

7. There is considerable debate in the contractualist literature as to whether hypothetical consent can ground norms. See Ronald Dworkin, *Taking Rights Seriously*, (Cambridge, MA: Harvard University Press, 1978), 37–53; Jean Hampton, *Political Philosophy*, (New York: Westview, 1996), 66; Hannah Pitkin, "Obligation and Consent–II" *The American Political Science Review* 60.1 (1966): 3952, 56. Cf. John Rawls, *Political Liberalism* (New York: Columbia University Press, 1993), 85. For a further overview of standard critiques, see Nicholas Southwood, *Contractualism and the Foundations of Morality* (Oxford: Oxford University Press, 2010), 135–137.

8. A significant point of debate in the social contract literature is whether the people the theorist imagines to debate rules governing their future interaction have a certain common moral makeup, such as a disposition to find common ground or ignorance about the interests of the parties they represent in dialogue. "Contractualists" hold for certain initial moral constraints about dialogue while "contractarians" do not place such restrictions on dialogue partners. The moral parameters of the contractualists ensures that the ideal dialogue results in moral principles, John Rawls, *A Theory of Justice* (Cambridge, MA: Belknap Press, 1971), 120. Contractualists can be further divided into those who conduct thought experiments involving idealized contractors operating according to ideal communication rules and those who argue that interpersonal morality is constituted by actual people debating according to ideal communication rules. The former group includes Kant; Rawls; John Harsanyi, "Morality and the Theory of Rational Behavior," in *Utilitarianism and Beyond*, ed. Amartya Sen and Bernard Williams, (Cambridge: Cambridge University Press, 1982); and Thomas Nagel, *Equality and Partiality* (New York: Oxford University Press, 1991). The latter group includes T.E. Scanlon, *What We Owe to Each Other* (Cambridge, MA: Belknap Press, 1998) and Jürgen Habermas, *The Theory of Communicative Action* (Boston, MA: Beacon Press, 1985). The benefit of the unconstrained nature of the contractarian dialogue is that dialogue partners are imagined to reach agreements that are in the parties' interests to respect regardless of the parties' level of desire to behave morally. Contractarians include Hobbes and David Gauthier, *Morals by Agreement*,

refer to even the last type of contract as involving hypothetical consent since the relevant theorists anticipate what actual people have rational grounds to endorse based on their self-interests. We need to engage in some kind of philosophical construct to model what large numbers of people would endorse since referenda on professional duties are neither feasible nor necessarily morally salient. The duties of security professionals need to be considered in reference to large numbers of people—all the people in the world—since service members or intelligence officers' actions can benefit all the inhabitants of their states and of allied states and potentially pose threats to the combatants and noncombatants of any state that threatens their state or allies or any state or region hosting irregular militants or pirates.

It is gratuitous to devote space here to defending one of the above contractualist theories first, because the collective moral responsibility grounds the relevant professional norms instead of hypothetical consent, and second, since I suspect[9] all contractual starting points would yield the same results regarding the contours of state agents' duty to facilitate a community's security.[10] A large group of actual people unconstrained by communication rules as well as a group of actual people so constrained might well endorse the same security-seeking tactics identified by the theorist based on a thought experiment involving idealized contractors and ideal communication rules since the options for professional duties for police and service personnel are fairly limited and the proper choices, whether one engages in egalitarian moral reflection or self-interested calculation, clear. Whereas the duty to assist the needy, respect people's privacy, or respect people's autonomy might be executed in many different ways in different contexts, inhibiting consensus on the constitution of such duties, the sorts of options we might put before real or idealized consenters regarding security-seeking norms are less numerous and less sensitive to cultural differences. Military norms, for example, turn on broad questions designed to produce clear action-guiding norms about the use of force such as "May military targets that are not vital to the attacker's strategy be attacked?," and "May military targets be attacked if there are risks to noncombatants?" We can readily predict how idealized or actual people would

(Oxford: Clarendon Press, 1978); Christopher W. Morris, "A Contractarian Account of Moral Justification," in *Moral Knowledge?,* ed. Walter Sinnott-Armstrong and Mark Timmons (Oxford: Oxford University Press, 1996), 215–243.

9. One cannot do more than anticipate what the second type of contracts would yield in its Habermasian construal.

10. Miller argues that state agents in democracies should be constrained in their pursuit of collective goods by the community consent embodied in local law, 248. He acknowledges that professional duties cannot also be considered moral duties if there are gaps between law and common morality. Therefore, I think that hypothetical consent does not suffer in a comparison with a reference to extant law as a moral guide, since Miller has to invoke idealized democratic law anyway to explain how institutional duties are also moral duties. Miller also refers to the teleological end of the institution to give content to professional norms guiding their behavior in areas left unspecified by law. My model provides state agents with a specific model for determining the parameters of their professional duty.

respond to questions involving their physical safety and so will not expect gaps between the anticipated consensus of a large group of people unconstrained by communication rules, people bound by egalitarian communication rules, and idealized consenters whose hypothetical consent is based on axiomatic preferences for the full enjoyment of their rights, and the like.

B. The Security Standard

Hypothetical consent can be used to expose the contours of professional norms and tactics by way of a formal framework I call the security standard.[11] The framework can be used to expose the contours of the professional norms of all the morally vital institutions, but I will here focus on governmental institutions tasked with maintaining the security of the state. Since government measures taken to protect people from rights violations usually include types of coercion, there is a risk that measures aimed at protecting innocent people will also violate those persons' rights. It therefore will not suffice simply to say that all protective actions by security services are permitted.

The security standard endorses norms and tactics. Within the professions, professional norms are general rules for institutional actors that are largely rule-consequentialist in their logic. The norms lead to the morally vital collective goods the institutions are designed to meet when all or most institutional actors adhere to the norms. Norms are morally rich as they deal directly with core human rights or moral goods. They are general, capacious, and communicative to practitioners and outsiders of the values of the profession.

Tactics are instrumental applications of norms and unlike norms, can vary with context. For example, the military norm of discrimination might lead to military units choosing lighter munitions or prohibiting indirect fire when confronting insurgents in densely populated areas. Discriminate tactics will depend on the physical environment, available technology, enemy behavior, and the like. Viewed the other way, the underlying and unifying principle of conscientiously chosen tactics is expressed in a norm. I will only focus on tactics in this chapter.

The security standard is composed of two major rules for picking tactics—two rules for expressing the contours of security-seeking state agents' professional duty. First, we can see that a rule would win the consent of all affected that directed state agents to adhere to tactics reliably, efficaciously, proportionally, and efficiently leading to the institutions' goals of security instead of tactics unreliably, inefficaciously, disproportionately, and inefficiently doing the same. Since security-oriented tactics ranking favorably in these four practical categories may infringe on people's rights, we can imagine consent accruing to a second rule

11. I apply the security standard to police tactics in *An Ethics of Interrogation*, chs. 2–3, 5 and to intelligence collection tactics in "Moral Concerns with Cyberespionage," in *Binary Bullets*, ed. Bradley Strawser, Fritz Allhoff, and Adam Henschke (Oxford: Oxford University Press, 2016), 251–276; "Intelligence Ethics and Non-coercive Interrogation," *Defense Intelligence Journal*, 16.1 (2007): 61–76.

selecting the most rights-respecting among the most reliable, efficacious, proportional, and efficient tactics.

With these two rules, the security standard endorses tactics surviving a three-stage winnowing process. The standard (1) canvases locally available tactics aimed at meeting the joint moral right of security; (2) isolates the most reliable, efficacious, proportional, and efficient tactics; and (3) endorses the most rights-respecting among the tactics meeting the practical metrics of (2). The practical elements of (2) are aimed at achieving the collective good of security while the deontological element of (3) acts as a brake, excluding practically effective tactics that come at too high a moral cost. Essentially, the security standard is a way of balancing affected parties' interests in the effective and efficient delivery of certain collective moral goods with the parties' interests in protecting other goods and rights potentially jeopardized by institutional actors' behavior.

Norms and tactics can "score" better or worse according to the security standard. A tactic with no conceivable causal connection to the end sought is imbued with zero justificatory weight. Some tactics are so brutal that the negative portion of a proportionality calculation can be assumed to outweigh any good done. A tactic that is efficacious only 10 percent of the time similarly fails the security standard. Such a low score on any of the criteria disqualify the tactic. In such a case, the state agents employing the tactic are not acting within the scope of their duties. A promising tactic has to be at least more efficacious and reliable than not (>50 percent) and must be proportionate. A tactic is proportionate if the harm done does not exceed the good accomplished or preserved through the action. Efficiency is context-dependent and so does not lend itself to a categorical or scalar assessment. The efficiency element has to be compared across different tactics and can potentially be a significantly lower scoring element than the other three without disqualifying the norm or tactic.

The rights-respecting element of the security standard is weighted greater than the combined practical elements, so a tactic that is reasonably successful in the practical sense can be excluded if it infringes on rights to a great degree. The basic calculation is that people cannot be modeled as consenting to a cure that is worse than the disease afflicting them. These are situations where the tactics meant to protect rights actually harm rights to a greater degree than they were being harmed or were likely to be harmed when the tactics were contrived. This is obviously going to be an inexact comparison since one needs to consider the impact of a security-seeking tactic, such as compelling plane passengers to pass through metal detectors, with the product of the calamity hopefully forestalled (terrorist attack) multiplied by the likelihood of its occurring. The implication here is that a given tactic might be consent-worthy in one environment but not in another, as the likelihood of certain kinds of rights violations changes.

Given a competitive total score, a contending tactic has to be compared against others. A lower scoring tactic is not consent-worthy if an agency can engage in a better-ranking tactic. The security standard provides moral grounds for people to constantly press for better tactics on the part of state agents, comparing their state's tactics with those used by agents of other states. State agents fail in their

duty if they persist in using outmoded tactics that are less practically effective or more rights-infringing than available alternatives.

The security standard endorses the extant phenomenon best meeting its criteria, giving legitimacy to security standard-compliant tactics already in use. Legitimate tactics are tactics expressive of state agents' professional duties, provided that state agents engage in these tactics in an upright manner. Obviously, state agents using permissible tactics for non-official purposes are acting outside of their duty (e.g., a soldier engaging in permissible collateral killing purely out of bloodlust or a police officer repeatedly charging his ex-wife with picayune traffic offenses).

In sum, the security standard answers the question for state agents: In what does my professional duty consist? State agents should use the security standard in assessing which norms to cultivate and which tactics to use. They should also constantly seek norms and tactics that are more reliable, efficacious, rights-respecting, etc. Legislators should hew to this standard when crafting laws meant to reform security agencies. The internal counsel for such agencies should interpret the letter of existing laws according to the spirit of the security standard. The public has a duty to use this standard to oversee the protocols of state agents dealing with foreigners (discussed in the next section). Tactics falling short of this standard, given economically and technically feasible alternatives available to the government, can be reasonably criticized and targeted for reform.

Hypothetical consent accrues to domestic government actions aimed at securing a domestic environment relatively free of rights violations. These actions include actions by military and intelligence operators aimed at defeating external threats to a state's security. There are two types of action, broadly speaking, of relevance to this enterprise: investigative and strategic. Investigative actions (undertaken by any sort of agency) approach targets who may be security threats in order to determine if they are in fact threats. These targets include domestic and international criminal suspects, foreigners who might have information of national security interest but who are not clearly identified members of foreign security agencies, and foreign civilians who may be irregular militants (e.g., insurgents, international jihadists). Strategic actions are actions taken against known adversaries such as foreign service members, intelligence officers, and clearly identified irregular militants. Strategic actions lack the tentativeness and gradualness appropriate with investigative tactics as they presuppose a clearly identified adversary; they are oriented to getting the best of that adversary.

Since all the people in the world can be modeled as consenting to a regime of outward-facing security-seeking actions, model consenters' (in one notional state) consent to foreign operations by their security services also potentially justifies action by foreign agents targeting them. This dynamic can best be explained by discussing its domestic parallel. Hypothetical consent is permissive when it comes to the justification of police tactics meant to keep model consenters safe. Considerations of how to secure the safety of consenters justifies a series of actions aimed at rights violators or potential rights violators. At the same time, a principle of reciprocity urges restraint of police tactics since it justifies police

behavior targeting the consenter if that person is suspected of perpetrating or planning rights violations. So the consent that we imagine people extending to domestic security-seeking tactics takes into account that they might be the target of those tactics. The same reflexivity must apply to outward-facing security-seeking tactics.

Regarding investigative actions, model consenters of one notional state must use themselves as reference points, asking whether they can consent to their state agents using tactics abroad that, via the principle of reciprocity, they must also permit foreign agents to use against them. Using this approach, the rule of thumb should be that security agencies should use the same investigative tactics abroad that they use domestically. For example, if the security standard indicates that warrants are necessary for a security service to intercept a domestic inhabitant's communications or that a domestic criminal suspect has to be warned about a right to remain silent in police interrogation, the same treatment should apply to a foreigner targeted by the security service. There might be exceptions if the foreign target is significantly different than a domestic one or if it is not feasible to extend the same treatment to foreigners as to domestic inhabitants. As examples of the former type of difference, the sophisticated encryption technology foreign intelligence officers use might prompt different monitoring tactics than appropriate for domestic criminal suspects. As an example of the latter kind of difference, certain types of up-close, manpower-intensive surveillance feasible for a domestic security agency might not be feasible in an adversary state. In this case, an intelligence agency might want to opt for satellite or drone surveillance—a tactic that might be more privacy-infringing since it permits seeing over walls shielding targets from street-level surveillance. If this more privacy-infringing tactic is consent-worthy under the security standard, the model consenter potentially permits her adversary's security agencies to do the same in her country.

The approach outlined here creates a universal norm for security operations. Foreign security agencies can be criticized for failing to meet the security standard when it is in their power to meet it. An example would be if an intelligence agency bugs the room of every foreign tourist, even though it is capable of targeting select foreigners of intelligence value. Regarding a similar concern, one might wonder if state agents should not adhere to local standards of security operations when operating abroad. This concern might seem particularly germane in cases when it appears expedient to treat foreign combatants or intelligence targets in a less deferential manner than domestic criminal suspects and the adversary state (where operations will occur) already treats its own people roughly. Yet one obviously does not want one's state agents using less reliable or less efficacious tactics (e.g., such as torture) abroad even if they are in a foreign state whose own security forces use less reliable and efficacious tactics. While one would want one's state agents to emulate foreign practices better than their own when operating abroad, practical limitations may make this impossible.

Regarding strategic actions aimed at state agents, we conceive model consenters are first as civilian benefitees of military and intelligence agency protection. The principle of reciprocity dictates that foreigners can benefit from the same protections, so model consenters consent to outward-facing strategic actions by their military

and intelligence personnel aimed at foreign state agents, with two limitations. First, military and intelligence tactics are only consent-worthy from the perspective of civilians if they can consent to being collaterally harmed by them when those tactics are targeted at their own state agents. Thus in a military context, tactics imposing a certain level of risk on foreign civilians are only consent-worthy if consenters can consent to the risk of being collaterally harmed when foreign militaries use the same tactics in operations in the consenters' homeland. So, for example, the security standard endorses the traditional tenets of jus in bello—just warfighting. Tactics must discriminate between military and nonmilitary targets, and not cause more damage than is warranted by the military value of a target. If people of one notional state can be modeled as consenting to other states' militaries deploying to war to defend their domestic inhabitants, even if the consenters' own state is the unjust aggressor, they would not consent to foreign tactics pursuing a just cause in an unnecessarily destructive manner, targeting civilians or causing more civilian casualties than are proportionally offset by the good of achieving tactical goals. (Proportionality is an optimal rule integrating two imperatives permitting both sides to pursue important tactical goals while minimizing collateral damage.)

This modeling exercise suffices to limit military and intelligence operations insofar as they affect noncombatants. One would also need to model hypothetical consent from the perspective of a military or intelligence professional in order to determine the limits of military and intelligence operations insofar as they affect state agents. This follows because state agents properly direct strategic actions at other state agents. In some cases, overlapping justifications would yield the same limitations as the noncombatant-based consent exercise. For example, noncombatants cannot be modeled as consenting to being directly targeted in military operations since such actions violate their rights[12] and service personnel cannot be modeled as consenting to directly targeting civilians because such targeting is neither a reliable nor efficient means of achieving a military victory (e.g., killing civilians instead of enemy service personnel leaves the enemy's military capacity intact). There would also be tactics failing the security standard that can only be modeled from a service member's perspective only germane to him, such as tactics using chemical weapons or napalm against massed infantry. I will not pursue service personnel-based consent-modeling further here.[13]

In all, the security standard prompts a cautious approach, particularly with respect to foreign operations, because a wide range of concrete practices could be justified if the security standard permits security services to conduct foreign operations employing the most reliable, efficient, rights-respecting, etc. tactics available to the service. The best locally available tactics justified by the security service will vary depending on a given state's wealth, size, technological prowess, and ingenuity. If the standard then effectively permits all security actors to "do their best," the standard

12. I am condensing a long argument here. Noncombatants' rights are violated because direct targeting of them fails the security standard.

13. I develop the security standard and its associated military norms in much greater detail in chapter 8 of the forthcoming *The Moral Status of Combatants*.

allows situations in which, for example, wealthy country A's intelligence services conduct very discriminate, sophisticated, targeted, and automated intercepts of foreign intelligence target's communications—so that very few innocent people have their privacy violated—while also permitting poor country B's intelligence services to conduct relatively crude, indiscriminate intercepts that violate the privacy of far more innocent people. So too in the case of war: the military of wealthy country A may cause far less collateral damage with precision munitions than the military of country B, despite the fact that B's military is trying just as hard to be discriminate and proportional. Thus, before engaging in a tactic promising a degree of collateral damage, an agency needs to consider if the inhabitants of its own state can be modeled as tolerating the levels of collateral damage associated with its adversary's reciprocal response. It could follow that that peer or near-peer adversaries might be permitted tactics a powerful state is not permitted when fighting a much weaker adversary.

II. IS PUBLIC SCRUTINY OF SECURITY OPERATIONS APPROPRIATE?

A. Dynamics of Oversight

Having articulated a moral standard for judging the operations of security operations, it is next important to consider the implementation of this standard. Is it enough for security operators to self-regulate according to the security standard or for their agencies to self-regulate through the actions of internal auditors, such as staff lawyers and inspectors general? Or must the public conduct oversight of these operations in order to ensure compliance with the security standard, or at least conduct oversight of the internal protocols and legal findings setting the parameters for operations?

In order to answer these questions, it is first important to clarify the practical dynamics of oversight relative to consent. It is a less pressing matter to assign and specify a duty of oversight as a distinct activity in cases of explicit consent when consent immediately precedes the contracted activity, such as the purchasing of an item at a store. It is also less pressing when consent is tacitly given throughout the duration of the relevant activity, since consent can be revoked at any time (by explicitly objecting), such as in the provision of a service involving the client's participation or active enjoyment such as an out-patient medical procedure, massage, or haircut, or in some consensual activity such as gameplay, debate, sex, etc. In these cases, oversight of the service provider's or activity partner's activities by a concrete, particular consenter is simultaneous or nearly simultaneous with consent to the activity. By contrast, hypothetical consent only creates abstract standards; compliance with standards has to be conducted empirically. In that case, concrete, particular individuals can and should offer their explicit consent to consent-worthy activities or explicitly dissent to activity failing this standard. So, from a practical perspective, government transparency is important since there is usually a lag between the execution of a putatively consent-worthy governmental

action and the effect on an inhabitant or foreigner. There will also be a significant number of people unaffected by government actions targeted at others. These temporal and participatory gaps inhibit real-time oversight concurrent with ongoing tacit consent. Therefore, just from a practical point of view, government transparency about its operations and post hoc review by some competent parties would be necessary to ensure compliance with the security standard. I will argue that this transparency—and the public oversight that comes with it—is not necessary to legitimize government programs but necessary to ensure that personnel in politically legitimate programs do not become corrupt or incompetent.

The legitimacy of national security actions comes from consent-worthiness in my theory, rather than the explicit consent of a state's inhabitants or citizens or openness to publicity. Explicit consent is not the source of legitimacy despite playing a paradigmatic role in social contract theory. Early social contract thinkers appealed to the notion of the consent of the governed to explain how a government's freedom-impinging actions could be consistent with citizens' freedom, despite the difficulty in explaining exactly how citizens or inhabitants transfer their consent to government officials. There are few opportunities for unambiguous explicit consent to government policies, and even the best candidates, such as oaths of citizenship or votes in referenda, prompt questions about the scope of consent and implications of being in the voting minority. Further, the popularity of a government policy does not necessarily have anything to do with its morality.[14] Therefore, if government transparency is necessary for the

14. The best (i.e., least ambiguous) candidates for expressing consent are ones that rarely occur. Signing a new Constitution, swearing an oath to one, or voting for one in a referendum are suggested as paradigmatic instances of consent to a government invoked in the classic notion of the social contract (John Locke, *Second Treatise on Government* § 89; Thomas Hobbes, *Leviathan*, ch. 17; Michael Walzer, *Obligations* (Cambridge, MA: Harvard University Press, 1970), xi). The obvious difficulty is that such events have not often occurred in recorded history (David Hume, "Of the Original Contract," in *Moral and Political Philosophy*, ed. Henry Aiken (New York: Hafner Press, 1948), 356–372, 362), and probably none have occurred with unanimous consent—a criterion the early contract theorists demanded (A. John Simmons, *Moral Principle and Political Obligation* (Princeton, NJ: University Press, 1979), 72). Further, it is not clear how being bound to one's ancestors' oaths or votes is consonant with the autonomy the doctrine of consent is meant to safeguard (Hume, 360). Immigrating and taking oaths of citizenship or naturalization would seem to express explicit consent (Harry Beran, "In Defense of the Consent Theory of Political Obligation and Authority," *Ethics* 87.3 (1977): 260–271, 262; C.W. Cassinelli, "The 'Consent' of the Governed," *The Western Political Quarterly* 12.2 (1959): 399; Walzer, xi), but most inhabitants of a country are born there and never participate in such events (Cassinelli, 398; Rawls, 13; M.B.E. Smith, "Is There a Prima Facie Obligation to Obey the Law?," *Yale Law Journal* 82 (1972–1973): 950–976, 960). Ritualistic performances such as swearing allegiance encounter difficulties of motivation, vagueness, and scope. Compulsory performance of such rituals cannot express genuine consent. If swearing allegiance is not compulsory, what sort of political obligation accrues to non-swearers? If the performance is voluntary, the ritualistic nature of the performance militates against the likelihood that participants grasp the contractual import of their mantras. Further, is one swearing allegiance to a particular leader, a system, or a particular canon of laws? If allegiance is sworn to the third item, this further argues against the prospect that consent is knowing, given the size and complexity of a canon of laws (Cassinelli, 402).

legitimacy of government programs, it is not on account of legitimacy stemming from inhabitants' explicit consent.

Let us now turn to the openness to publicity standard. This standard of political legitimacy would reject any policy that could not be revealed without destroying its efficacy. Many contemporary exponents of the standard draw from Immanuel Kant's signal articulation of the idea in *To Perpetual Peace*. Kant argues that "all actions that affect the rights of other men are wrong if their maxim is not consistent with publicity."[15] He means that an action is immoral if the general rule guiding the action cannot be known by all without that widespread knowledge making the execution of the action impossible. Performing the action would be impossible because the action's success inherently depends on the maxim (the general rule guiding the action) remaining covert in the way that a lie's success depends on its remaining covert or because it would necessarily create universal opposition in the manner of a person's announcement of his policy of murdering anyone he dislikes. Laws compliant with this publicity standard must be accessible to inhabitants, that is. they could actually go to a library or the internet and read the statute. An attendant feature of permissible positive law is that the law would not necessarily create opposition once it was studied.

Policies need to be *open* to oversight on this line of thinking in order to meet the conditions for citizens' consent (they do not actually need to meet with their consent, for the reasons already articulated). Concealed policies are not even candidates for political legitimacy because of an absence of the conditions necessary for citizen endorsement of the actions—even if the law would have been popular.[16] By way of analogy, a man wrongs a woman if he has intercourse with her while she is too drunk to give informed consent, even if she would have given her consent if sober. David Luban convincingly argues that Kant's openness to publicity principle[17] does not preclude all forms of secrecy. "First-order secrets" cannot be revealed without frustrating the action or identity the secret is meant to conceal, for example, "John Smith is actually an undercover officer." However, "second-order secrets"—secrets about secrets—can be revealed without destroying the relevant first-order secret. "The police department utilizes undercover officers" can be publicly disclosed without jeopardizing undercover operations and without creating necessary public opposition. It therefore passes Kant's openness to publicity principle.[18] Since the second-order secret passes the principle, the related first order secret may be permissibly concealed on

15. Immanuel Kant, "To Perpetual Peace," appendix II, [381] 135, ed. Humphrey.

16. David E. Pozen sympathetically outlines this view, "Deep Secrecy," 62 *Stanford Law Review* 257 (2010): 286.

17. I will use the term "openness to publicity" to express the political application of the publicity principle. The broader publicity principle embedded in the Categorical Imperative captures an aspect of the possible universalization morally sound maxims display: they can still be efficacious even if universally known.

18. David Luban, "The Publicity Principle," *The Theory of Institutional Design*, ed. Robert E. Goodin, (Cambridge: Cambridge University Press, 1998), 154–198, 191.

Kantian grounds. However, a relevant third order secret such as "the government will keep all police activities secret" cannot be revealed without creating public opposition—since this gives the government unchecked power[19] and abnegates duties of inhabitants described below.[20]

I do not find this reading of the openness to publicity standard compelling in all cases because I can think of (and will discuss below) intuitively permissible security-seeking tactics that lose their efficacy if the *fact* of their use is revealed. These are second-order secrets that need to remain secret in order to be effective. The security standard can justify their use. All this will be defended further below, but for the sake of argument now we will entertain the possibility that the existence of some government programs is legitimately kept secret. However, since the personnel assigned to a program are vulnerable to groupthink, blind-spots, corruption, nepotism, and perverse incentives, proper guidance of these programs can only be promoted with external oversight of some sort. Thus, I will proceed below, taking a practical view of the openness to publicity standard as the relevant rationale for public oversight. On that view, external oversight or the possibility of external oversight is not constitutive of a program's legitimacy, but important in order to ensure that legitimate programs do not become corrupt. Section III will address the obvious tension between the need to oversee a program that cannot persist if its existence is publicly revealed.

B. The Public's Interest in Oversight

We can now expand on the idea that government programs practically need external oversight in order to ensure compliance with their moral authorizations. Again, government programs (inclusive of their personnel) are not self-monitoring and do not win real-time tacit or explicit consent from state inhabitants. Who should perform this oversight? The public has interests, rights, and duties relevant to oversight of government security services that would be trespassed if state gents err, overreach, or become corrupt.

First, an inhabitant has an interest in ensuring that his own rights are not being violated by the government. One is obviously in a privileged, though still fallible, position to judge whether one is being wronged by another. Some might also term this interest a duty, though duties to the self—such as a duty not to be made servile—are less widely recognized than duties to others. This duty to the self can be supported by an associated duty to others in the following way. It is likely that the government will perform the same rights-violating actions against others if one does not protest the government violating one's own rights. Thus, allowing the bad behavior to continue unchecked fails to protect others.

One also has a right to oversee government activities for the reason that a contracting party has a right to see the work he has purchased. A taxpayer has

19. Luban, 191.

20. Pozen refers to the concealment of second-order secrets, "deep secrets," and regards them with deep distaste because the public does not even know to ask about them, Pozen, 274.

a right to see the services he subsidized with his tax monies. The purpose of this type of oversight of government actions is to combat fraud and waste.[21]

Regarding duties, inhabitants of liberal states alienate certain powers to state agents to use on their behalf. Principals are morally responsible for their agents' behavior when that behavior is consistent with the principals' orders so the principal has a duty to ensure that her agent is doing things she is morally required to see accomplished and not doing things she herself is morally forbidden to do.[22] This applies both to direct agents, who do relatively low-skilled actions the principal could have done herself such as gardening, babysitting, and proofreading, and to free agents, highly skilled actors such as lawyers or accountants the principal relies on for their expertise and ability to make independent judgments.[23] Obviously, the moral impetus for the public to oversee state agents is greater than the impetus to oversee private agents because of the potential harm these free agents can do utilizing the powers of the state.

There are two specific duties the public has to meet when overseeing state agents. First, people have a collective moral responsibility to contribute to a secure environment, a responsibility largely met when they contribute to the creation or sustaining of relevant state institutions.[24] A component of sustaining state institutions includes ensuring that state agents are indeed working to secure this kind of environment.[25] Second, since the coercive means state agents use to prevent rights violations perpetrated by state inhabitants against each other can themselves violate people's rights, the public must ensure that its agents are pursuing the end of security in ways conforming to the security standard. In other words, the public has a duty to ensure that its agents pursue the moral end of security (creating an environment relatively free of rights violations) without violating deontological concerns making state security morally valuable.

21. These points are famously made by Jeremy Bentham, discussed by Amy Gutmann and Dennis Thompson, *Democracy and Disagreement* (Cambridge, MA: Belknap Press, 1996).

22. A principal is not responsible for something her agent did completely of his, the agent's, own accord, having nothing to do with the agency transferred to him by the principal.

23. Free agents bear a heavier burden of independent moral responsibility than direct agents for electing tactics the principal does not have the training to fully understand. Practically, principals can usually not exercise real-time oversight of free agents because of a lack of relevant expertise, and so will likely focus on consequences, which are intelligible to a layperson in a way tactics are not. Oversight will then likely be expressed in reform efforts rather than proactive guidance. For example, the average civilian, supportive of a given military operation, does not have the expertise to decide what weapon systems should be used in a particular attack, but can demand to know if some more discriminate tactics or technology is available after a large number of civilian casualties are incurred in an operation.

24. This might sound strange, but another example of a negative duty creating a subsidiary positive duty would be a the duty not to harm others leading to a positive duty to ensure one's car is in good working order, one's gun is securely locked, and one's pool is fenced.

25. Other relevant positive duties include paying taxes and complying with all but egregiously unjust laws of any state one lives in or visits.

Since the behavior of state agents abroad can incur responses from foreign state agents, it is in the public's self-interest and consistent with their concern for their neighbors to oversee their agents' behavior and object to unnecessarily provocative or otherwise immoral behavior abroad. Assuming that behavior abroad potentially creates a reasonable foundation for in-kind foreign responses, the public should object to practices that exceed the security standard marking what they would tolerate being done to themselves. This limitation has to be considered in kind rather than degree, given that a certain kind of operation releases the adversary government from engaging in the same kind of operations even if they can only perform it in a cruder fashion than the first government. Thus, for example, the public should object to their security agencies intercepting foreign civilians' private communications electronically if they are unwilling to countenance less-sophisticated foreign agencies doing the same to them by steaming open envelopes.

III. IS THE PUBLIC COMPETENT TO OVERSEE SECURITY OPERATIONS?

The public has a duty to oversee state agents, yet may not be competent to execute this duty. Usually, duties imply the duty-holder's power to perform the duty but this is not always the case. For example, one may find it hard to observe the duty not to unjustly harm others when operating a new vehicle or tool and learning too late that it is difficult to control.

In many cases, the general public is not competent to technically assess the internal protocols of security agencies. One would often need as much knowledge as an expert practitioner to know if a weapon system, a computer code, or interrogation technique is the most reliable, efficacious, proportionate, efficient, and rights-respecting available. However, the general public is competent to assess whether the effects of a given tactic raise moral concerns. For example, the public does not know if stopping and frisking random young men in high crime areas is really the most efficient or reliable method of inhibiting gang violence, but does know that this tactic is disruptive to neighborhood life and offensive to innocent people accosted by police. This concern is enough to begin a conversation with state agents about whether this tactic really is the best available, and if so, whether the good done is really worth the harm.

In order to assess the actions of state agents, the public needs a good understanding of not only the actions of state agents but of the threats the agents' operations are designed to meet.[26] For example, one cannot assess the proportionality of a response unless one understands the danger being faced. Concerns related to the public's knowledge of state agents' operations will be addressed in Section IV. The public's being informed about the threats security agencies are trying to meet creates a different problem, particularly in the international arena. In some

26. William E. Colby, "Intelligence Secrecy and Security in a Free Society," *International Security* 1.2 (1976): 3–14, 9.

cases, a detailed picture exposes sources and methods of intelligence gathering to the state's adversaries.[27] The adversary can learn about the threat-publishing state's technological capacities such as its satellite or other aerial reconnaissance resources (and flight paths), based on the imagery released, and its signal intercept (SIGINT) capacities, based on the electronic communications released. This knowledge both helps the adversary prepare to destroy or jam those assets in case of war and helps the adversary hide the strategic assets that have been shown to be vulnerable. More dangerous still, is the direct threat posed to undercover operatives or their intelligence assets who are the sources of the sensitive information describing the foreign threat. There will be sensitive programs in the adversary state's defense and intelligence apparatus known only to a few, and the process of elimination conducted by counterintelligence agents when such programs are compromised can be brutal and swift.

So there will be times when a government would need to describe a threat in order to justify expenditures or operations at a level of specificity it cannot use without jeopardizing sources and methods of intelligence collection.[28] These are moments of irreducible tension between the need for oversight and the security aims civilian oversight is meant to secure. A government's concealment of a sensitive threat assessment amounts to a third-order secret: a secret policy justifying keeping secret a program encompassing secret operations. Again, Luban does not think concealing third-order secrets can be justified as it gives unchecked power to officials.[29] I recognize the risk in permitting third-order secrets, but think external oversight should be omitted in this case where oversight meant to check compliance with a standard threatens to contravene the goals of that standard. My reasoning follows below. By way of analogy, extensive standardized testing of students should be curtailed if it gets in the way of their education. Again, according to my theory of political legitimacy, lack of oversight does not inherently nullify legitimacy. Lack of oversight is a practical, rather than a constitutive, problem in that it creates risk of corruption.[30]

Whether the keeping of these kinds of third-order secrets—the revelation of which would compromise important security standard compliant operations—is itself in keeping with the security standard is difficult to assess. Keeping these secrets is obviously an efficacious and reliable way of preserving operations that would be compromised by publicity. Efficiency seems to be a non-applicable variable. Proportionality is hard to assess given all the relevant unknown variables.

27. Thompson notes this possibility in Dennis Thompson, "Democratic Secrecy," 114 *Political Science Quarterly* (1999): 186.

28. Thompson, 182.

29. Luban, 191.

30. I think the security value of these secrets outweigh the Millian values Gutmann and Thompson argue are associated with public debate about government actions: the promotion of political cooperation in the face of disagreement that comes from the possibility of consenting to governmental actions, the promotion of citizens' moral perspectives, the extension of respect between disagreeing citizens, and the self-correcting nature of deliberation, 100–101.

Keeping the secrets is not *obviously* disproportionate, comparing the benefits promised by the program with the disvalues of omitting the truth to the public and running risks of corruption.

Regarding the rights-respecting element of the security standard, the public generally has a right to know what its government is doing in its name and so any kind of government secret would seem at first prejudicial to the public's rights. This right to know is relevant to the protection of other rights since government programs failing the security standard may be abusing more substantive rights among the people affected. Yet clearly, there are limits to the public's right to know. The public does not have a right to know personal information about government employees such as their medical histories or financial details (with the possible exception of top elected officials). The public does not have the right to know first-order secrets that will endanger state agents. State agents have an institutional right linked to their professional roles to be spared from unnecessary or frivolous endangerment by their own governments. Their rights trump the public's general right to know about government programs when it comes to particular agents' involvement in the program. Yet we cannot simply conclude that it does not wrong the public to conceal third-order secrets in order to protect the agents involved because the program may be doing the public such a disservice due to its practical inefficacy and disregard for human rights that a proportionality calculation indicates that the good done by exposing the program outweighs the disvalue of exposing agents to harm. To be clear, this is probably a rare case where the mere revelation that a particular type of program exists would expose agents to risk (whereas usually, second-order secrets such as "the police use undercover officers in counter-narcotics operations" can be revealed without exposing particular agents to undue danger).

If the program is security standard-compliant, then the security standard indicates that its existence can be permissibly concealed because of the risk to the state agents involved. Ideally, if responsible members of government recognize that the program is a failure, they will pull their agents from the field, halt the program, and announce to the public what went wrong. Failing official measures, a whistleblower would ideally alert field agents before revealing the program or only reveal the program if agents were not currently deployed, counting on the government's subsequent protection of the agents from possible foreign reprisals. Failing all those ideal scenarios, a whistleblower may reveal the program to the detriment of field agents if the proportionality calculation is strongly in favor of revelation.[31]

The other justification for concealing third-order secrets is that revelation would lead the adversary to close otherwise fruitful intelligence-gathering channels. I have argued that the purpose of publicizing government programs generally is to give the public an opportunity to verify that the programs are

31. In particularly odious programs, agents' right not to be endangered may be offset by their culpability in immoral actions they should have known were immoral and inefficacious, for example, torture.

security standard-compliant. Advocates for the concealment of third-order secrets regarding security standard-compliant programs are effectively holding that the government should be trusted with designing security-seeking programs and then unilaterally determining whether their existence should be concealed. Skeptics worry that all programs need to be publicized (even while keeping tactical applications secret) in order to avoid corruption. Roughly, it seems that concealment of third-order secrets violates the rights of the public if the program is being corruptly run but does not violate their rights if concealment facilitates a vital and properly run national security program. Revelation of the latter type of program would in fact fail the government's duty to protect the public. The problem, of course, is that secrecy prevents the public from knowing which situation obtains. We need some kind of publicly available data to use to model the consent of all affected parties to the concealment of third-order secrets. I will tentatively conclude that concealment of third-order secrets passes the rights-respecting element of the security standard if there are significant national security threats facing the state. We can model all affected parties as agreeing ex ante to a premise permitting a state facing significant national security threats to engage in third-order secret keeping—effectively, to engage in secret government deliberations about which programs to initiate based (ideally) on the security standard and which programs will have to be concealed from the public.[32] Barring a clear, present, and significant danger, it may well be too risky to give a government the power to conceal third-order secrets.

If we go down this road, the government's knowledge of certain threats will have to be kept secret, as will the intelligence-gathering operations meant to assess the threats; and the contingency plans developed to meet them. The expenditures on personnel and equipment designed to counter the threat would also have to be kept secret if their nature is so specific as to tip the hand to the adversary, for example, if country A buys chemical-resistant suits for all its service personnel, adversary country B will realize that its secret chemical weapons program has been exposed.

State agents have to operate on their own recognizance in cases where third-order secrets are legitimate. This situation does open the door to corruption and abuse and so necessitates the careful vetting and training of recruits to security agencies. Disclosures of sensitive threat assessments and secret operations *would* be indicated by the security standard if corruption and incompetence hindered state agents from actually securing their state.[33] An imperfect compromise designed to mitigate the tension between security and oversight would be to have an oversight body of legislators assigned to the agency who themselves

32. This consent extends to targets of intelligence collection, who can be modeled as consenting to their own government engaging in reciprocal intelligence collection and secret-keeping.

33. This argument creates a standard for whistle-blowing. Revealing threat assessments or programs whose efficacy depends on secrecy is not appropriate, but revealing gross abuses by state agents in the prosecution of these programs may be appropriate, provided one meets some criteria similar to those appropriate for civil disobedience.

were sworn to secrecy. This option is imperfect because overseers committed to secrecy have no legal way of alerting the public or their colleagues outside of the select committee if the security services ignore their concerns and the wider legislature does not act on their necessarily vague, unclassified recommendations.[34]

IV. WHICH GOVERNMENT PROGRAMS ARE PROPERLY KEPT SECRET?

Section III broached the key question of this chapter: what types of government actions are properly classified and kept out of public view? We now have a formal answer implied by the foregoing discussion of threat assessments. Operations, expenditures, recruitments, protocols, internal legal rulings, and threat assessments meeting the security standard but which cannot be revealed without jeopardizing the relevant operations should be classified. This section will specify the programs meeting this criterion. A surprising number of military and intelligence operations can be revealed to the public, at least at a certain level of generality, without harm to national security. In order to make substantive recommendations about what sort of secrets should be classified, I will consider five typical activities of intelligence agencies and three typical activities of the military. I will assume that some tactics within these categories can meet the security standard without working out specific justifications. Analysis of concrete activities will produce five stock rationales arguing for, or against, secrecy.

SIGINT—the key question to consider when judging security operations is whether disclosure of government actions will directly or indirectly endanger state agents or civilians and whether disclosure will lead adversaries to cease activities from which the government is currently garnering useful intelligence. Cyberespionage is consistent with public disclosure at a certain level of generality (i.e., second-order revelations). It can be revealed that state agents attempt to collect classified information from adversaries' computer networks and even that a particular foreign agency is targeted. This follows, because, in the digital age, every technologically-sophisticated state assumes its adversaries are attempting cyberespionage and every such state is engaged in cyber defenses including encryption, information assurance activities, and intrusion and malware detection. I will call this assumption that the adversary is already engaged in defensive operations the Defense argument. First-order disclosures that would compromise a specific operation should remain secret, for example, "agents posing as defense contractors plan to use zip drives infected with the XYZ virus to install a back door in the Quds Force network this July."

Secrecy is appropriate with respect to more traditional SIGINT involving the collection of communications via the interception of various kinds of microwave and other electromagnetic transmissions. Disclosure of a state's ability to capture certain kinds of transmissions can lead to their enemy halting usage of that technology, such as al-Qaeda's alleged halting of satellite phone communications

34. Pozen makes a similar point, 332.

after the media revealed that US agencies could monitor the calls and also use their signatures for targeting purposes in 1998.[35] I will call the adversary's abandonment of tactics in reaction to its enemy's abilities the Avoidance argument. This is a key example of a program that I believe passes (or could pass)[36] the security standard but the existence of which must be concealed lest the purpose of the security standard not be met. Revelation of the second-order secret that the United States is intercepting al-Qaeda satellite phone calls makes the program inefficacious. This is the case even if the adversary has no choice but to use the form of communication in question, because they will presumably communicate less than they would have otherwise. The need for secrecy is mitigated to a degree if the intercept capability is understood to be less than comprehensive such that the adversary can wager that there is a reasonable chance that his communication will slip through the collector's net (call this the Randomness argument). Once it is widely known that an agency can collect a certain kind of communication signal, secrecy is still appropriate regarding operations collecting transmissions from particular targets. Al-Qaeda closed down a communication channel after it was leaked that NSA monitoring had led to an intercepted order from Aymin al-Zawahiri to al-Qaeda in the Arabian Peninsula leader Nasser al-Wuhayshi to attack US embassies in the Middle East.[37] It should also be noted that while SIGINT raises privacy concerns, the elimination of SIGINT as an intelligence source forces agencies to rely more on human intelligence (HUMINT). HUMINT is far more fraught than SIGINT in that it involves the penetration of undercover agents into enemy territory, the corruption of foreign intelligence assets, the enabling and financial support of criminals, and the interrogation of detainees.

HUMINT—the most traditional occupation of intelligence officers is "turning" intelligence assets, that is, convincing members of adversary states with access to security-sensitive information to reveal the information. Secrecy about HUMINT operations is unnecessary on a general level because of the Defense and Randomness arguments. Publicly revealing that undercover intelligence officers from state A are attempting to turn assets in state B tells state B nothing it did not already assume and was not already attempting to root out with its own counterintelligence operations. Secrecy should be maintained with respect to specific operations along the lines of "an intelligence officer posing as the Agricultural minister from country A is attempting to turn Gen. X in the Strategic Air Command." Obviously, both the undercover agent and the prospective intelligence asset are endangered by disclosure. Assuming that the undercover agent is

35. Whether the leak directly led to al-Qaeda's change in procedure is contested. Cf. "Bush Account of a Leak's Impact Has Support," David E. Rosenbaum, nytimes.com, publ. December 20, 2005 and "File the Bin Laden Phone Leak Under 'Urban Myths,'" Glenn Kessler, washingtonpost.com, publ. December 22, 2005.

36. As noted in Section III, a civilian has a limited ability to assess whether a given operation has better available tactical alternatives.

37. "Qaeda Plot Leak Has Undermined U.S. Intelligence" Eric Schmidt and Michael Schmidt, newyorktimes.com, September 29, 2013.

conducting a just mission, his life is of moral value apart from the inherent value of all people; his being compromised puts his state at greater risk (this is the case even if he fails in his mission but is able to escape safely). I will call this the Danger argument.

Covert Operations—paramilitary operations conducted by undercover (i.e., nonuniformed) operators including assassination, incitement, and sabotage—bear some similarities to HUMINT operations. General disclosure that agents may conduct covert operations in an adversary state is permissible because of the Defense and Randomness arguments. Specific disclosures are forbidden because of the Danger and Avoidance arguments. The Danger argument would apply in all cases while the Avoidance argument would be particularly apt in the case of sabotage, such as when state A ensures that the rare components for some weapon system or computer network procured by the adversary security services are defective or contain listening devices or malware. The adversary would know not to install the components if the plan was disclosed.

Interrogation—there is an argument to keep interrogation tactics secret because adversary agents may be able to prepare for them, thus reducing their effectiveness. This argument is more germane for non-coercive stratagems than coercive tactics (which do not pass the security standard anyway). It would be useful for security agents or irregular militants to know that interrogators of their adversary typically engage in certain kinds of emotional manipulation, for example, playing on detainees' fears, sense of loyalty, resentments, etc., or that interrogators offer fake incentives, for example, promises to assist detainees' family members or to forgo sentences in exchange for information. However, the Defense and Randomness arguments suggest that disclosure is not overly problematic. Knowing that adversary interrogators might play on detainees' concern for their families or comrades does not eliminate the fact that detainees will be concerned for their families and comrades. Given that emotional backdrop, even the savvy detainee who is dubious of the interrogator's attempts at rapprochement might seize on the possibility that *this* interrogator is telling the truth about helping family members or minimizing the suffering of comrades.

Cryptography—the fact that a security agency tries to break its adversary's codes can be revealed because of the Defense and Randomness arguments. The Defense argument can justify disclosure of attempts to break the encryption of particular networks so long as the adversary already knows that other states are aware of the network. For example, disclosure that agency A is attempting to break the codes protecting the computer networks of its adversary's nuclear facilities is permissible but not if the adversary thinks its nuclear program is still clandestine. As with SIGINT, specificity may lead to the adversary closing down networks protected by insecure encryption.

The following three subjects pertain to the military.

Battleplans—standing contingency plans can be disclosed at the level of generality where they would be obvious to potential adversaries, for example, a Russian tank invasion of the Fulda Gap will be met with NATO armor and air assets (the precise number of assets used should remain classified). There is also little incentive to keep secret even less obvious plans from weaker adversaries who do not

lack the resources to respond to the battleplans. For example, there is no reason to keep secret, contingency plans to attack an adversary with stealth bombers if neither the enemy state nor its allies have any way of detecting these bombers (call this the Asymmetry argument). Otherwise, specific battle plans for imminent operations must be kept secret because of the Danger argument.

In certain cases, foreign aggression can be deterred through an adversary's ambiguous plans for response. Chinese officials might suspect that the United States will not really go to war to defend Taiwan, but the possibility that the United States would may be sufficient to deter aggressive moves to restore Taiwan to mainland control. Noninterventionist plans should be kept secret in cases where deliberate ambiguity serves as a deterrent to hostilities. In a similar case, plans to omit reciprocal responses should be classified if deterrence is maintained by the adversary's logical assumption that a certain action would earn a reciprocal response. For example, British ballistic missile submarines are said to have handwritten notes from the prime minister with orders of what the captain should do if Britain is attacked with nuclear weapons. It is appropriate to keep these instructions classified since adversaries' reasonable assumption that British submarines would retaliate in case of nuclear attack serves to deter a rational adversary.[38]

Deterrence maintained by false, explicitly announced policies is a harder case. For example, in the run-up to the Gulf War, the Bush administration supposedly made it known to Saddam Hussein through diplomatic channels that a chemical attack on Coalition forces would be met with an American nuclear strike. I suspect this was a false threat. There are obvious moral concerns involved with a government lying to its own people if a false threat is made more publicly. There is a considerable literature on this subject raising some of the above-mentioned issues regarding government secrecy, which I will not address here except to touch on a point relevant to the security standard. There is less impetus to disclose the truth about a covert false threat if the ultimate rationale for government transparency is to reform policies inconsistent with the security standard. This is because the actual policy is not inconsistent with the security standard. Whether the policy of making false threats to adversaries is consistent with the security standard depends on its prudence. While lying to an adversary may initially seem less problematic than lying to a domestic audience, false threats may increase tensions and make the adversary more aggressive and more entreprenurial with its intelligence operations. Yet one can also imagine cases where lies are prudent instances of deterrence.

Troop movements—in cases of active hostilities, troop movements have to be kept secret because of the Danger argument.

Location of military assets—during peacetime, the location of strategic assets designed to deter a peer adversary, such as Cold War-era American and British ICBMs, has to be kept secret on account of the Defense argument. This argument also applies to any military assets in active theaters of war. The location of assets designed to deter or to respond to weaker adversaries often do not need to be

38. Luban makes a similar point, 164.

classified because of the Asymmetry argument. For example, the drone operators stationed at Creech Air Force base in Nevada, engaged against operations against the Taliban in Afghanistan, do not need to fear an enemy lacking any expeditionary capabilities.

V. CONCLUSION

In liberal states, security services should seek to secure an environment relatively free of rights violations to inhabitants by using the most reliable, efficacious, efficient, proportionate, and rights-respecting tactics available. This standard undergirds just coercive actions by state agents and should guide internal reviews of policies and interpretation of relevant law. The public has a duty to oversee the activities of government security agencies in reference to the security standard. Nonetheless, the security standard takes precedent over oversight in cases when disclosure would neutralize the efficacy of security-seeking tactics. Secrecy is indicated for government policies meeting the security standard when revelation of these policies would directly endanger state agents or indirectly jeopardize national security by drying up intelligence sources. These areas of secrecy open up opportunities for corruption and abuse, risks that can partly be mitigated by oversight from a select group of citizens (legislators, judges, perhaps even ordinary citizens who have security clearances). These select committees are imperfect solutions to the basic tension between security and secrecy because their inability to disclose their privileged information limits their ability to end immoral or wasteful programs when they are in the minority of their committees or when the security services ignore the committees' objections. I believe this tension is an irreducible risk attendant to liberal societies, akin to the possibility of intolerant religions flourishing under a government guaranteeing freedom of religion or illiberal parties coming to power in a democratic process. The solution to the security dilemma, as in the other inherent difficulties of liberal systems, is the cultivation of the virtues of citizens and public servants.