Three Legs Consortium *Working Paper on National Security*, No. 2
[September, 2019]

Debating Digital Diplomacy
Perspectives on Strategic Propaganda in National Security

Prof. Makumi Mwagiru
Adjunct Professor of Diplomacy
School of Humanities and Social Sciences
Strathmore University
Nairobi

&

Mwotia Makumi, MA
Three Legs Consortium
Karen

TABLE OF CONTENT

Introduction

The discipline of diplomacy operates in a dynamic world. Diplomatic practices serve the discipline as it interacts with that dynamic environment. As a result, diplomatic practices have always reflected changes that happen whenever the hinterland of the discipline is extended.[1] This extending of the discipline is always marked by new themes of diplomacy. Over time these have been for example peace diplomacy, economic diplomacy, border diplomacy, diplomacy of the diaspora, and environmental diplomacy. These extended diplomacies do not exit from the discipline: they instead form sub-disciplines. These extended diplomacies extend the terrain of diplomacy and its content. And this in turn requires diplomatic practice to adjust itself to accommodate these new hinterlands of the discipline.

A new trend in the growth of the discipline of diplomacy that encompasses a new challenge for diplomacy and its practice has lately emerged. This new challenge for diplomacy has been branded 'digital diplomacy'. It reflects emerging challenges prompted by the dynamic world in which diplomacy operates. It reflects some of the dynamics of the growth of information and its technologies: what has been called the 'information revolution'. While its' antecedents are not new, its' trend is. And it is from this that the newness of digital diplomacy is distinguished. Developments in new forms of communication in the earlier parts of the 20th century led to changes in the practice of diplomacy. Those changes required diplomacy to emerge from older practices in which diplomatic communications were inhibited by the slow means available. With faxes and telephones, diplomatic communication became faster and more immediate. But the communication revolution also meant more far reaching changes. They meant, with the advent of radio and television that information was more readily available to all people.

These changes had repercussions on the face of diplomacy. They meant that since information was more readily available to everybody, diplomats were no longer the only sources of information about foreign affairs and political and other developments in other countries. These

developments posed challenges for diplomacy. In particular, they required diplomacy to make a new claim for its *niche* in state and international affairs. Diplomacy responded by adjusting aspects of its practices to accommodate the new developments. This gave rise to a new form of diplomacy, public diplomacy. It was especially realized that diplomacy needed to be engaged in communication with publics and not just governments.

In the second half of the 20th century even more far-reaching developments took place. There were even newer forms of communications like television and the internet and all its devices. These emerging forms of communication made information as readily available to people in villages as it was to publics in the capitals, capitols and in government. There was hence an information revolution. This revolution meant that there was a surfeit of information. It challenged further the practice of diplomacy. Since now most of the information was in the public domain, diplomats were no longer the sole source of information. They needed to develop further practices by which they could come to terms with this surfeit. In addition, information is now being shared more easily through new technologies - digital means, which governments have little control of. While the provenance of the information is not always known, it is accessible to anybody with the digital means.

In the face of these developments, the challenge for diplomacy and diplomats has thus become greater than the mere sorting out of the massive new information, and its analysis. The challenge is that this information has short temporal frames, but reaches unprecedented numbers of consumers. The challenge is that while that information is immediately superseded by new information, the mind-set created by the earlier ones is already become set. And yet, some of this information – disinformation – is harmful to the national interests and national security interests of the state. It needs to be countered, but within very restricted time frames. Traditional diplomatic practices were not set for this state of affairs. Therefore they have to adjust to the new digital technologies, to enable diplomacy to play its rightful role as one of the sources of power of

the state. This problem is also compounded because the sources of this new information are not always – indeed hardly - known. These developments have enlarged the hinterland of public diplomacy. They mean that diplomacy needs to be involved not only with the huge amounts of information available, but also with dealing with its effects on public mindsets. It is realized that the information could change public perceptions about issues that concerned decision makers, and about developments in other parts of the world. Shaping that information has hence became an important tool of diplomacy: at its operational and also strategic levels. And since this can only be done by resorting to the same tools as the creators of the information, diplomacy must resort to the same tools to counter the information peddled. And to do so requires it to 'dirty its hands' by entering into the digital arena.

This paper notes the uses of new media as a strategic tool for states. It inspects the new type of diplomacy that has emerged: digital diplomacy, and states' attitudes towards it. The paper argues that the new media have posed challenges for the practice of diplomacy. They have required that diplomacy – and all its supports like intelligence services – engage in countering changes in public perception about issues that happen in the new media. Both states and non-state actors make use of the new media as important strategic tools. They do so through propaganda and disinformation. This propaganda and disinformation have serious consequences for national and international security. The paper argues that states need to take into account various aspects of the new realities in responding to the new media. There must hence be more concern with the strategic uses of the new digital media, and its legal, ethical and policy implications for national security.

Approaches to Digital Diplomacy

As noted earlier in this paper, the information revolution has challenged the practices of diplomacy. The practice of diplomacy and its conceptions has been challenged in the face of other developments in the international system, and its changing interests. This has happened in the face of developments in knowledge and appreciation of the environment, about

human rights, about territorial borders, about bio-technology, climate and climate change and others. In response to the various developments, diplomacy has had to change and develop new foci about its practices. Sometimes there has been universal appreciation and acceptance of the issues at hand. More often however, those that believe in the importance of the new developments and their role and effect in the international system have had to popularize their acceptance as aspects that should be reflected in the practices and mental frame of diplomacy.

The acceptance of digital diplomacy as one of the emerging practices of diplomacy is no different from this trend of the discipline's response to issues arising in the temper of the contemporary international environment. Like others, there are those who have subscribed to it, and those who resist new developments. The view that propaganda and disinformation, and their use of the contemporary devices of information technology should be embraced in diplomatic practices is one of the views, and schools of thought about how and whether governments should use these media as bases for protecting and promoting national interests. This view is shared by both the intelligence community [IC} and also some diplomats. It is one view in other words of how states should react and respond e.g. to digital diplomacy.

The other view and school of thought, reflects what is its view about digital diplomacy, and its effects on the practice of diplomacy, and on construction of the state, and the ways it challenges the traditional role of diplomacy as the constant alternative to war. In this view this traditional role of diplomacy has been challenged by the unregulated digitalization of information and communication. It is shared among others by Bjorn &Pamment.Its basis is that there has been a digital revolution that is still going on apace. The problem in this view is that developments arising from the information revolution like fake news, disinformation by state & non-state actors and weaponization of information "have raised fears of digital technologies having unintended consequences that may undermine…the social fabric of western societies."[2] [note: their concern is with the effect of digital diplomacy on western states]. But they further argue that

> "…the 'dark side' of digital diplomacy…the use of digital technologies as information and propaganda tools by governments and non-state actors in the pursuit of strategic interests, has expanded to the point that it has stated to have serious implications for the global order."[3]

They maintain that diplomats and foreign policy makers embrace it, but also try to find solutions to countering it. They need to counter it because:

> "if basic understandings of the social reality are systematically falsified and reshaped to serve the foreign policy interests of the day, then the epistemological foundation that allows diplomats to bridge some of their differences simply collapses. The digital construction of 'alternative realities', that is, of public frames of social interpretation loosely linked or utterly unconnected to verifiable facts and evidence-based reasoning, becomes a form of undermining confidence in societal institutions and, by extension, in the diplomatic sphere, an ominous prelude rather than an alternative to war."[4]

In the view of this school of thought, digital media technologies disrupt "the way in which information is generated, circulated, interpreted and used…but also ensured that digital propaganda, that is, the deliberate attempt to disseminate information on digital platforms with the purpose to deceive and mislead is here to stay."[5]

This debate is about how to respond to the challenges caused by the information revolution and its appurtenances. The debate is joined because "there is clearly a major problem as, with a few exceptions, many [governments] simply do not have the necessary capabilities to react to, let alone anticipate and pre-emptively contain, a disinformation campaign before it reaches them."[6] This means that the debate and the contending views that frame it can be stated more clearly and in unambiguous terms. These are whether states should regulate this digital growth arising from the information revolution; or whether states should accept its existence and ubiquity, and join it in accordance with its own rules that have developed.

Contextualizing the Two Approaches

The emergence of these two schools of thought about digital diplomacy and whether states should embrace it in their diplomatic practices are founded

on two competing world views. These two world views reflect also the contending views about the international system, whose purpose it serves, and who should create the rules that guide it. These are also the views that emerged in the aftermath of the second world war, and the style and rules of the international system that were created.

The second school of thought has a clear conceptual view of the world and the standing of the actors involved. Hence its concerns are with the threats posed by the digital age and associated *bricolage* like digital diplomacy, to the fabric of *western* societies. The concern of this school is with the threats to the "global order". For Africans this global order means the order that these western societies created for Africa at the Berlin Conference of 1884/5. That order was informed by certain views of the relationship among actors in the international system. In the intellectual foundations of that order the world borrowed heavily from the epistemology of Charles Darwin as implemented socially in the thinking of Herbert Spencer was divided between those who were strong, and could therefore be able to survive, and those who were weak and could not survive. And those that could survive were to use force – through the colonial process – to reproduce themselves in other parts of the world. This process of western reproduction in other parts of the world was later called the internationalization of world society.[7]

The view of diplomacy of this school is with the traditional diplomacy of states and among states. This diplomacy is being threatened by being made to engage in unsavory things like 'digital diplomacy', over which they have little control. There is no appreciation that the expanse of diplomacy has increased to also involve non-state actors [i.e. track 2 diplomacy], and that the challenges for that type of diplomacy is to become sustainable for it to survive in the contemporary world.

The first school of thought on the other hand is concerned with current realities. The current realities are for example that non-state actors like perpetrators of violent extremism, terrorists and the like have come across a platform that tends to equalize them with states - or even make them

more effective. Therefore in the view of this school, if you can't beat them, join them! And hence: counter them with the same tools they are using.

This school does not sit and complain that its official diplomats are dirtying their hands engaging in activities like digital diplomacy that unfriendly non-state actors like terrorists use: like digital technology and social media. It asks its diplomats and others to develop tools of being more effective than those that the violent extremists use. Hence the suggestions of going beyond counter-narratives, and understanding the emotional mind frames of the victims of violent extremism at whom responses are aimed.

Indeed, the essence of the approach of second school and its rationale is heavily western oriented. Its basis is that there is currently a threat posed by "one of them" i.e. Russia and that this is what they should address in all its dimensions. That school has little to do with countering violent extremism in Africa or Asia: just with it as it affects the west and seen from the context of their post-cold war society. They need a new enemy: and they are busy finding it in the person of the old, cold war enemy, Russia. That school has surveyed the emerging world; and in doing so it has realized that the "others" have been equalized by certain things like the developments and opportunities offered by modern technology. It feels that it cannot be able to control the use of the corresponding resources, and hence feels threatened. It would hence prefer more controls of these media [and preferably a control that puts them in charge].

The second school fails to realize that the old post-second world war world and its structures are changing – and have changed rather rapidly especially after 9/11. They have not come to terms with these changes. It also does not realize – or accept – that following the end of the cold war, the west created enemies [like terrorists] and thus the war on terror as a frame in which to have something that took over the cold war framework that had been the controlling framework for half a century. It needed new enemies on which to hang its strategic frameworks upon. The problem is that these new enemies rely a lot on structures and frameworks that are easily available to everybody, and at virtually no cost. They are fighting enemies in the new contemporary world that exist in their own

imaginations. Hence their efforts to ensure that some countries – that were irrelevant in the cold war period – do not develop nuclear weapons.

That school finds the new realities of a power – a soft power – available freely difficult to contemplate. Their world view is of a world that ceased to exist. The world view sees developing countries as things to be influenced by the enemies of the west [i.e. Russia]. Hence the parametres of its responses:

> "A broader history of public diplomacy is required; one that acknowledges its role in shaping foreign societies' development as a form of soft power. hostile states will argue that Westerners have meddled in their societies for centuries, influencing their elections, institutions and citizens through public diplomacy techniques mixed with diplomatic and economic levers and occasional coercion. Digitization has simply provided a more level playing field, at least temporarily, in which digital platforms may be exploited at relatively low cost. As the wealthiest countries dedicate increasing resources to closing the exploits in their systems and shaping societal resilience, one wonders where this leaves developing countries. It is conceivable that this period of high-profile influence campaigns within Western countries is the prelude to something far more disruptive to the developing world, which could have far-reaching consequences for global security."[8]

Clearly this is the world view that the piper of the funders of research in the west would like propounded, as intellectual support for the west in the post-cold war cold war, on whose one side is the old familiar, but diminished enemy, whose new platform for fighting this war is the opportunities offered by the age of digitalization. And like in the old cold war the "developing world' are mere tools and victims of the post-cold war cold war. This is why these countries must not borrow the idea being sold that the way to fight the threats in which the current problems is through finding a way to kill or control digitalization [an impossibility], but to engage it on its own terms: not to quit the kitchen!!

It needs to realize that war in the new world is asymmetric. And this war will not be won by using the tools of symmetrical warfare. Militaries cannot win it; and so the challenge is to adapt to the new realities of an equalized world. And these realities must embrace the challenges of

digitalization; and learn to use it in their diplomatic practices. And more than anything else it needs to realize that diplomacy provides one of the important tools for using propaganda and creating counter- disinformation strategies that need to be invested in the tools of the state as they confront the national security challenges embedded in the information revolution.

Propaganda, Disinformation, and Intelligence

Propaganda and its art and science has evolved a lot in the past two decades. The trends show that it has taken shape beyond the traditional state-sponsored propaganda, and engages a wider group ranging from non-state actors to individuals. Despite this enlargement of the actors involved, their objectives and scope vary greatly. The identity of the non-state actors has also changed: and some of them for example operate in the guise of public relations firms;[9] these are often hired by governments to support the state organs like ministries and diplomatic missions.

The common denominator in issues dealing with propaganda and disinformation is tied to the technological boom, and by extension its new devices commonly known as social media. Traditionally, states create and manipulate social media accounts and feed different forms of information that they consider important for public consumption. This creates an unmatched platform for state government propaganda and levels of disinformation. However, this trend has slowly dissipated with the increase of alternative news and alternative access to the various forms of information sources. These have degraded the state propaganda toolkit.

Amongst the national sources of national power, the military has for long used proxy warfare to increase their operational efficiency. They have done so through using externally available resources, including those with specialized skills like ammunitions, resource mobilization, field combat and others. In the 21st century a flood of opportunities have emerged both for states, but also for non-state actors. These have used proxy warfare to attain similar goals. They have for example used dark web entities whose skills include network penetration and influencing public opinion through mobilizing the social media.

Russia has for example perfected this trend. It has strengthened its use of propaganda and disinformation campaigns. In its region, the victims of its state sponsored propaganda include Ukraine. Beyond its region its victims have included the USA, whose presidential elections it is thought to have manipulated. Other countries like China thrive on the use of disinformation and propaganda to manage internal criticisms, and control internal perceptions. The end-state of this resort is to promote sympathy and develop positive attitudes to the ruling party.

The increasing challenge of propaganda and disinformation has also been felt in Africa. States there have used social media in the attempt to enhance the functioning of politics within the states. Although the 'Arab Spring' has highlighted this development in some areas of Africa, this trend has happened across the different parts of Africa, and is not restricted to one area of the continent. In the continent, the role of Intelligence has changed the manner in which strategies for dealing with the suppression of propaganda and disinformation domestically and internationally are perceived. From this perspective, the role of intelligence communities has emerged as being inter alia to shape the domestic and international image of governments. This is in turn intended to promote and maintain a level of trust in the population, and also give governments a certain, positive international standing globally.

Disinformation campaigns tend to thrive in environments where the immediacy of information and the need for the authentication and clarification of received information are contentious and highly uncertain. Traditionally, the primary sources of information like television networks were housed by media companies. These sources of information, including radio and newspapers were trusted sources of information because they were the only alternative sources of information beyond official, government sources. In these instances, these alternative news competed with other alternative sources. Hence the catchy headlines and phrasing that dominated the marker space of the 20th century.

The natural response of governments to disinformation ingested by the public from alternative sources was to impose strict controls over

traditional forms of information providers like television stations, radio stations and newspapers. However, the perception arose that the media was under government control, and that it was restricted by law in terms of the information that it could disseminate. For this reason, public trust in this media eroded. As a result, a vacuum arose, and other forms of alternative media entered the scene. These new alternative media increased openness and accessibility through the digitalization of the platforms. There has thus been an infusion of alternative sources of information open to the public. All this meant that even if governments shut down privately owned media stations, there were many alternative sources of information. But then, government strategies have also been forced to change. They no longer have to use the old forms of control like shutting down media stations. They can for example allow the media to cover things – like the 'inauguration of the 'peoples president' in Kenya, as a different strategy. Had that 'inauguration' been banned, other alternative media would have covered it anyway, causing loss of trust in and support for the government. This was clearly what the inaugurators hoped for since they were steeped in the traditional history of government responses to such events. They lost that battle.

The war on terror has significantly changed the way the alternative sources of information are used as strategies. Terrorists have shown themselves able to be resilient and to adjust to the changing operational environment. They have to do so in order to survive and be able to carry out their activities. They have been able to fill the information gap that has been created by the public's craving for alternative narratives and sources of information. They have been able to create and own television and print media outlets as tools for spreading propaganda and furthering their political and ideological goals. But it is not just terrorists that have done this. States too have adopted similar strategies. The case of Djibouti in its current completion with Kenya for a seat in the UNSC is a good case in point.

As all this has been happening, there has evolved an even deeper distrust in governments. This has increased demands for protection of the rights to privacy. As a result, platforms have enhanced their privacy

capabilities by ensuring users of increased privacy and protection of their identities. In doing so, these platforms have been used by non-state actors as tools for radicalization.[10] This has become a credible national security threat because of its vast audience reach: even in schools whose students have become ideal candidates for radicalization. The further danger is not only that terrorist organizations like *Al Shabaab* and ISIL advancing their online strategy. The danger is that as a result of the massive doses of disinformation, publics are confusing propaganda for knowledge; and as a result, these alternative 'truths' have become catalysts for political tension and instability.

Information, Knowledge and Perceptions in the New Media

The information revolution now means that information readily available to everybody in the world. The ready availability of information means that there is also a universal surfeit of information, normally characterized as an information overload.[11]That surfeit of information is not however, by itself the problem. The problem is how that information is presented and to what purposes. In the new realities of the international environment, that information has been used to shape and change perceptions of its receivers. That information is used by both state and non-state actors to fulfill different goals. Since the new media is open for the use of all actors, it has been used in ways that have had intended and unintended effects. It is still being used heavily for example in promoting violent extremism. In this usage it targets different users and changes their perception towards other individuals, groups, and towards states.

This perceptual change in public mindsets that is entailed in the information has severe consequences for national and international security. How states and other actors relate to it determines their ability to manage it and its effects in various spheres. Understanding the dynamics of this information surfeit is therefore very much of the essence. The basic epistemology of this understanding is that information and access to it by themselves do not constitute knowledge. Knowledge comes from what its receivers do with it, and how they perceive it and relate to it. How that

information is processed in turn affects the consumer's view of reality. In this setting, the creators of that information are able to change the perceptions of the consumers of that knowledge. They are able to change their world view, and their perceptions about social, political and other relationships.

The creators and interpreters of that information have thus been able to shape and change the information environment. Where those creators and interpreters have agendas different from those of governments, they can and have caused serious disruptions of the stability and security of states. This has been the strategy of terrorists and terrorist groups like *Al Quaeda*, *Al Shabaab*, ISIS and others. They have, through their manipulation of information been able to change the national, regional and international security landscape. This is, in essence one of the aspects of the war on terror.

But then, this sort of process is not only undertaken by non-state actors. Practitioners of diplomacy who vent against being engaged with non-state actors now confront the reality that they must in this setting confront also state actors using digital technology for propaganda and disinformation purposes. The challenge for nay-saying diplomatic practitioners is that this new environment also means countering similar actions by state actors. A recent development in the competition between Kenya and Djibouti for a seat at the UN Security Council illustrates this. In that competition, the African Union had voted about which between Kenya and Djibouti will represent the Eastern African region at the UNSC. A substantial number of AU members voted for Kenya. Djibouti refused to recognize this vote. In a news media outlet, Djibouti claimed that it "*slightly* lost votes to Kenya in the AU."[12] The votes were 37 for Kenya and 13 for Djibouti, hardly a slight majority. Djibouti also linked the UNSC seat to the maritime conflict between Somali and Kenya. It says that if Kenya won the seat it would "undermine Somalia" and affect the region.[13] The issue in this election is no longer the grand strategic issues that the country will pursue if elected. The issue is the disinformation [slightly victory] and the propaganda [undermining Somalia]. Mindsets have already been changed.

To counter this, the response should be aimed at the level at which that mindset was addressed. This level is the emotional one of one state using its offices at the UNSC to bully/undermine another. And the creator of that disinformation and propaganda was a state; and it was addressed to resident ambassadors to Djibouti. The issue is whether diplomacy can claim it will 'dirty its hands' in countering such state-driven disinformation and propaganda against it.

The creators and interpreters of information use disinformation as the major tool of achieving their strategic aims. States, one of whose major aims to secure their citizens and territory must respond to this threat created by disinformation. While they cannot possibly control the dissemination of this information, they can respond to it in various ways. One of the ways in which they can do so is through propaganda and disinformation. Since these are the tools used by the creators of information, states must meet the challenges of that information through similar means. These similar means include propaganda and its countering, and disinformation and its countering. They do so through their organs and agencies, the most important of which are their diplomatic organs and security agencies.

To do so effectively, these organs and agencies understand, or must, that there are two aspects of that information that are of the essence. That information is a source of knowledge, but it does not itself constitute knowledge. There is therefore in this matrix the potential knowledge that the information can create. There is also crucially, the perception of reality that ensues from that knowledge. This knowledge and ensuing perceptions are what must be countered through propaganda and disinformation. Propaganda and disinformation are old strategies in human affairs. They have for long been realized to be crucial strategies and tactics in war contexts. And war contexts have always relied on propaganda and disinformation to do so. The challenge for many strategists has been to use them in non-war contests. One such context is their use as an accepted practice of diplomacy. While diplomacy has relied on intelligence as one of its tools, this aspect has been 'hidden' because practitioners of diplomacy

considered themselves to be above using what they viewed as unsavory means to meet the ends of diplomacy.

But then, diplomacy must confront the realities of the international system. And the reality is that the information revolution has enabled actors to "subvert reality."[14] This subversion happens through the means of propaganda and disinformation. It:

> "illustrates how the fundamental goals of managing the collective attitudes of [populations] by the manipulation of significant symbols has endured. This manipulation allows for the creation of policy contestation both domestically and internationally where none previously existed. It takes facts and makes them fictions and preys on the conditions and foundations of how humans make decisions. The significant manipulation of information can skew cognitive biases and alter propensities for the acceptance of risk and reward."[15]

Information, Subversion of Reality and National Security

The subversion of reality by actors – state and non-state – fundamental poses problems for national security. It does this because it can have various effects. It can for one, affect decision making in national security. This happens because the national security decision makers are also consumers of the information peddled through the various modern media. It can also affect policy responses to issues arising in the operational environment. This essentially means that it can affect perceptions about the national security operational environment. And the effecting of perceptions about that environment can in turn affect and even shape the trend and direction of national security policies that are designed.

Thirdly the subversion of reality can affect citizens' relationship with their own government. Affecting citizens' relationship with their own governments is and has been engineered by both state and non-state actors. States have for example used it in pursuit of their [foreign] polices about regime changes in other states in their operational environment. Non-state actors have used it to destabilize governments, and hence making it possible for terrorist agendas to take root and be accepted. The various "springs" that have happened – the "Arab Springs" [including

Sudan], the "Hong Kong spring" currently unfolding and the reported fear of Russian government that citizens may begin to "Arab spring" about elections that have taken place - are evidence of this. And finally the subversion of reality can affect perceptions of citizens of other countries about others. The propaganda and disinformation happening about the Somalia/Kenya maritime conflict can affect perceptions of decision makers in Kenya, in Somalia, and the perceptions of both countries citizens; and the perceptions of third parties and their citizens about the conflict.

Djibouti's disinformation about the intentions of Kenya at the UNSC was addressed to decision makers of the sending states whose ambassadors were addressed by its minister for foreign affairs. It was aimed also at affecting the policy responses of those governments especially when the UNSC membership comes for voting at the UN. And most importantly, it was aimed at the Somalia citizens, and was intended to affect their relationship with Kenya regardless of how the International Court of Justice decides the maritime issue. And, given the large number of Somalis in Kenya, it was also addressed to them. This has serious national security concerns for Kenya, whichever way the conflict with Somalia unfolds.

Dynamics of Responses to the Subversion of Reality

The information revolution is largely unregulated. Its' effects of subverting reality in countries is also equally unregulated. While states have individually come up with laws and polices about it, they cannot, in the nature of the dynamics of the information revolution and its tools fully achieve any meaningful regulation. Nevertheless, the subversion of reality poses serious threats for states and their national security. While there may not be much they can do about the revolution and its direction short of stopping it - which is impossible – they must somehow respond to its dynamics.

Since the challenges of states are different, their responses to the challenges involved depend on the realities of their operational environments, and also to the resources they have at their command. States do not enjoy the same resources. But it is also accepted that no state

has at its command all the resources it would need to address and respond to all possible threats. Hence whatever the response of states, they are constrained by the fact that their resources are not infinite. Nevertheless, there are some basic elements of state responses to the subversion of reality that ensues from the information revolution.

One objective characteristic of responses is that the speed of their propaganda and dis-information activities is of the essence. This is because of the temporal between readers or viewers of information and their mental response to it. There is a clear relationship embedded in what people read or see, and what they believe. In this relationship what they first read or see forms the basis of what they believe. This is a psychological response that is firmly embedded in human consciousness. The challenge for those responding to the subversion of reality is that once embedded in the consciousness, it is very difficult to undo or counter-act. There are many examples of this in Kenya that happen especially in cases of disputed presidential elections. In that aftermath, there is always [dis]information about police killings, including the use of live bullets and killing innocent children. The problem is that that is the reality that enters the sub-consciousness of consumers of that information. The information is repeated, thus deepening consciousness on the sub-conscious. And in that way, the information becomes 'knowledge'.

This dynamic means that there are two challenges that those responding to the subversion of consciousness face. The first is clearly that there are issues that arise in the process that must be responded to. The second is that having made the decision – which is a policy decision to respond – they must counter-act to the propaganda and disinformation, or both, that those subverting have engrained. The challenges faced are informed by the very essence of the process of creating propaganda or dis-information. These are essentially process issues. And because they are process issues, the realities of the process must be borne in mind. The realities are that the effect of the information revolution is that there ends up being a surfeit of information, coming from very different and often unrelated sources. And because of this surfeit of information, its receivers

find it more difficult to distinguish what is accurate and what is inaccurate information.

For these reasons, the process of countering propaganda and disinformation does not begin with skewing the information available. This is indeed virtually impossible because of the surfeit of information available. Logically therefore the process must begin with re-orienting the information. In this process it is necessary for:

> "a targeted individual or state to self-select or privilege certain information. By playing on a host of socially and culturally conditioned attributes as well as cognitive biases, a propagandist is able to feed the public's voracious appetite for information, even if the information is entirely fabricated."[16]

The issue of Kenyan Somali citizens being profiled in the war on terror is a clear example. The challenge was to identify the "culturally conditioned attributes and cognitive biases" being addressed by the propaganda, and to respond by addressing the same attributes and cognitive biases. Providing figures and long histories cannot do the job at hand.

Successful propaganda or responses to disinformation happens if the false or misleading information is combated. Success in this dynamic, means that the propaganda information becomes part of domain of accurate and transparent information that is available to its receivers. This is how the process of reversing the manipulation of information that its creators intended. This is the whole psychological dynamic of countering and re-orienting information. It is important especially in the digital environment in which the information environment takes place. Receivers of information have a very short time to absorb the information before they move on to another source of sometimes the same but often of different information. The aim therefore is to ensure that the receiver's mind does not shift perception from its focus on "the world as they think it is"; this is the temporal dynamic of the process: to prevent the reorientation [i.e. corruption] of the receiver's "social & cultural foundations".

This is the challenge. It means that in order to succeed in propaganda and dis-information processes, the responders minds must be

conditioned by two things. They must first understand their intended audience. Without doing this it is impossible to design any propaganda and counter-disinformation measures that can work. A responder from Japan or any other foreign environment cannot therefore come to Kenya and pretend to be able to respond in the context of the Kenyan social and other environments. The whole counter-process involves challenging "the audience's foundations for thinking". This means understanding what they think about themselves, about events happening and being made to happen – for example terrorist attacks etc. To understand that audience of receivers of information, responders must know them fully. Fully knowing and understanding them requires knowing them as well as they know themselves; and even better knowing them "more than they know themselves." The essence of this psychology is that:

> "by pulling on the strings of identity that combine to make individuals and groups who they are, their orientation can be manipulated. Successful propaganda subverts reality and calls into question the foundations of knowledge."[17]

It has been observed that current approaches where countering violent extremism in the social media is seen as a simple matter of offering counter-narratives are problematic.[18] In this perspective for example, narratives of violent extremism appeal not just to their content but also to emotions. Therefore CVE approaches should counter those narratives with others that similarly address the emotions, and offer compelling and contrasting images to those used to draw supporters of violent extremism. This entails "moving to the broader aesthetics of communication and not just to the logic of the message". This is best done by using aesthetic media "in a way that resonates, symbolically, culturally and emotionally, with the audience that is being sought."[19] Thus:

> "future online CVE counter-narratives should first be communicated through aesthetic media. These should serve to summarize aspects of the narrative being communicated and should resonate, symbolically, culturally, and emotionally with the audience that is being sought...this content should invoke positive emotions in order to gain high levels of

> engagement…those conducting CVE activities should listen to, and tailor their content to their audiences and engage with dialogues rather than simply publishing content."[20]

From this perspective, countering violent extremism and the narratives used to do so, is a much more complex matter than merely telling youth at risk about counter-narratives and the true statements of religious doctrines. The challenge is to identify where the narratives of terrorists are able to reach the 'solar plexus' of youths they are in the process of radicalizing.

Framing Formulation of Laws, Policies and Ethics

States are not going to one day wake up and decide that they will end the information revolution. The information revolution and all its *bricolage* like digitalization is part of the process of the growth of human knowledge. It was also not something that happened overnight: indeed it took almost a century for it to reach the heights that it has now breached. But this does not mean that states should not and cannot address it. They can. The issue is what they address. Since they cannot stop it, they can only address some of its consequence, and in the process make the environment that their citizens breathe a little fairer. At the same time, in doing so states must appreciate that the revolution is part of the developing interdependence of states [that some people beautify by labeling it "globalization". Being a source and consequence of interdependence, there is no possibility of any individual state developing laws and policies and strategies that are not harnessed in common with what other states are doing. The information revolution is internationalized – indeed globalized. The biggest threat of the information revolution is security – national and international. Therefore states need to develop an international information revolution peace and security system, that resembles what Mitrany developed long ago, and what he called *A Working Peace System*.[21]

States response to the information revolution – and to its handmaiden of digitalization - happens along three frameworks: that of the law, policy and security. But cross-cutting all these responses are ethical

responses. Legal responses are probably the weakest responses to the problems and issues related to digitalization. Their weakness is derived especially from the fact that responses to digitalization often touch on the fundamental human rights of citizens, and people generally. Some of the human rights that are touched by such responses are fundamental human rights. As such there is a limit to what states can do to address the problems. Besides legal responses must always go together with recalling the injunction most strongly stated in the South West African cases: that human rights are not given by states, but are inherent.

Policy responses are the strongest ground on which states can stand in designing responses to digitalization. They are important responses because they prescribe the policies that states need to adopt in addressing issues related to digitalization. They are especially important because they can, if designed properly, address and include the participation of citizens in responding to the multiple problems that are groomed by digitalization. Polices however, must be implemented otherwise there is no use formulating them in the first place. Indeed the problem with many countries has not been the lack of policies: it has been having multiple policies about all manner of things that have never been implemented, or indeed cannot be implemented. Thus the formulation of policies must also go together with the design of strategies to implement them. And in turn, strategies themselves must be implemented because unimplemented policies mean unimplemented policies. To implement strategies there also need to be doctrines, which are the implementation arm of policies. This triad of policies, strategies and doctrines is the ultimate response to digitalization and its problems and challenges. And to be effective this triad requires, always effective public participation.

Legal responses and policy responses must both the servants of ethical considerations. The reason for this is that laws and policies that do not take into account the ethical dimensions are unlikely to be effective or to be effectively implemented. The ethical dimensions are especially important if states address digitalization through national security policies [and strategies and doctrines]. The ignoring of the ethical dimensions of

laws and policies eventually leads to their being impossible to implement. And laws and strategies that cannot be implemented or are, for ethical reasons not implementable amount at the end of the day to zero plus nothing.

Legal and Constitutional Issues

Responses to digitalization through the law raise many important issues. They do so inter alia because the problems associated with digitalization are surrounded by the realm of a grey area between what information is allowed and available, and the limits of the law in addre3ssing them. And at the bottom of this issue are always the rights, granted by constitutions about the human rights and entitlements of citizens.

One of the major problems with digitalization is that it deals with information that is openly available to the public. This is in security terms called open source information. There are masses of such information available to anybody with access to the media that can access them. Open sources cannot be closed in democratic societies. And indeed attempts to so would not meet the approbation of the court system. And neither can the intelligence community be required, or even be able to spend resources scanning all information and its diverse sources. That would be a task that would even leave Sisyphus confused and breathless. Tracing the sources for attribution is an impossible task in the digital age. This is all compounded by the problem that the information in itself is not harmful or a danger to security or anything else. The problem is with interpretation of the information by its providers and by the recipient. And yet there can be no law proscribing giving certain interpretations to such information. There may be in societies that resemble George Orwell's *1984*; but societies like Kenya have moved away from that form of political and social organization.

Possible legal regulation always has some criminal responsibility element. But in the digital environment, it is difficult to attribute criminal responsibility, and even harder to attribute it to any specific individuals or individual. While it true that there are many actors that have hostile intentions to the state and its citizens, it is difficult and even impossible to

trace all of them. The problem with them is that they have no fixed abodes and not addresses – much less emails that can be traced to them. They operate in networks that have no borders. While clearly they have local agents in the domestic environment – and law enforcement agencies are able sometimes to trace them – only a few of them can be discovered. It is necessary to have laws that deal with such supporters. But these will always be short reaching laws, and may not be able to address the larger context. Besides the law cannot always have the means of tracing radicalized individuals because its concerns are with what the human body does and not what is in the human mind – and heart. And equally difficult is the issue whether the law can proscribe an individual's engagement with the knowledge of the science and technology that is involved with digitalization. Indeed, states spend huge resources precisely the acquisition of such knowledge because it is used in the service of the public good and national interests.

Hard liners in many countries suggest that the law can be used to proscribe the sources of digital information – and its distributors; and this eventually would lead to proscribing the users of the technology. Those aligned to this view even suggest that the private sector should be compelled to support governments' efforts to do this. It is even suggested that the civil society should also be brought within this frame of approach. But all this runs contrary to guarantees about human rights that are enshrined in constitutions. It also does not take into account that engaging the private sector in this kind of endeavor would threaten other equally important policies of states like encouraging private investments in the country. Quite clearly, this approach to the law does not take proper account of its limitations especially in a free society. Besides this approach does not take into account – or fails to remember – the problem at hand with digitalization is that it knows no territorial boundaries. And the jurisdiction of the law only applies to the territory of a state and not to those who are outside it.

Besides all these issues, digitalization of information operates in a very hazy area between what is lawful and what is not. And at the same time

laws, especially criminal law – and tax laws – may be enforced, but at the risk of creating disaffection among citizens. This would eventually make the legal approach counter-productive. It would do so because it is especially in the climate of such disaffection in society that enemies of the state and citizens thrive on. At the end of the day, a fractured society with what seem to be effectively enforced laws would create a haven – and heaven – to those that are an immediate threat to national security.

Policy Issues

The policy response to the problems of digitalization is probably the best one. It is preferable because its thrust is much less coercive than the legal one. Besides good policies, properly conceived are more likely to attar public support and participation. To be affective however, policies require a sound running theme: they require a guiding philosophy. Without such a philosophy, policies are likely to look attractive and even be embedded in elegant language, but be completely ineffective. Similarly, the strategies that are meant to implement the policies must also have a theme and a rationale that stands the test of scrutiny. The main theme for example of embedding counter-terrorist policies needs to be clearly articulated also that it can attract the support of the major implementers, who are the citizens. The problem is that sometimes policies and strategies are devised and created within offices, among officials who at best only imagine what the interests of the citizens are, and even worse what specifically their participation should be.

Policies sometimes also do not have a clear idea to whom they are addressed. Some of them proceed on the intellectual frame that they are addressed to those that threaten national security. The problem is that *Al Shabaab*, for example unlikely read such policies and strategies; and if they did they would not care because their operational philosophy is not earth bound but bound somewhere else. Deterrence has never worked if the person or entity that is the subject of deterrence does not care much or at all about the deterrent threats. Addressing the wrong addressee is like threatening a hundred year old person with the ultimate threat of death.

The best enforcers of policies and strategies on the problems of digitalization – for example dealing with terrorist threats – are the citizens. Citizens are indeed the first and last frontier of the implementation and hence effectiveness of such policies. Policies and strategies aimed to do that must clearly articulate the full participation of the citizens and explain the importance of burden sharing in the enterprise. And besides this, proper citizen participation in such policies and their implementation means specifically that: the burden of participation and even its decision making must rest with them. A policy or strategy in whose citizen participation is only a small percentage of the overall participators is not useful and will never be effective. A policy or strategy in a county that prescribes say a hundred participants, but the bulk of whom are officials is not a well conceptualized policy or strategy. It indeed belongs to the famous bookshelf in decision makers' offices and not to the operational environment.

For example, the best approach in which to address the narratives that terrorists employ in radicalizing citizens is to have not just a counter-narrative [this can surely be done in offices] but to have one that addresses the emotion and soul of the intended recipients. But the emotions and soul of the recipients can only be discerned by the community itself because it best understands itself. This cannot be taught in universities and is not contained in any textbook. It cannot be contained in these because it is a dynamic phenomenon that is living: and it lives in the particular society. It certainly cannot be imported from the capital – or capitol.

All these issues exist in the context of the proper framework of the war on terror. In that war, the public needs to feel that it is engaged in a war. Strategies of how this can be achieved are the issue at hand. The rationale of this happening is that if the public knows it in war time, it is willing to make concessions even about its freedoms etc. If it does that, it will clearly be a better partner in combating the war on terror. The problem arising in the war on terror – anywhere – is how the feeling and knowledge of engagement in a permanent war-time can be established, especially where the enemies actions are intermittent [although deadly]. In other words: the

issue is how to ensure that the public does not see the war on terror and consider it to be "the government's war"[22] rather than one in which the whole society is engaged.

Ethical Issues

Ethical issues run through and surround all these issues regarding the legal and policy frameworks. In the ethical framework the controlling basis is the standing of the state and how it promotes and projects that standing. Many of the problems given rise to by digitalization are about great things like national security and social and political values like democracy and citizens as foundations of the state. In this frame of thought, the state must hence not make itself the major rationalizing factor of its own enemies. Thus requires that it conducts itself with democratic and accountable probity; and maintain always the high democratic and law abiding moral ground. Among the other inhabitants of that ground is the participation of citizens in framing and formulating the laws and policies proposed.

The moral high ground includes also the treatment of citizens in the policies proposed. In Kenya at some point in the war on terror there were parts of Kenyan society that felt that they were being profiled. To understand the target audience as much or better than it understands itself, there arises the moral dilemma: asking citizens to behave like the target audience in order to understand it better; while at the same time targeting it as an audience. And besides, if counter-disinformation approaches show too many fissures and social fractures, the issue is what will happen to the society itself in the face of the problems and issues being addressed. It might cause fractures in the society. And those could give more comfort and room for the enemies, who will thus have more room to operate.

Ultimately, it should be remembered in the framework of laws and policies that national security policy centres around foreign policy. It does so because the operational environment that national security operates in is extremely dynamic and VUCA. National security is also eventually about the existence of the state. And the state exists in the environment where all the other states. Existence is an external operational dimension issue.

Therefore all these policies and laws are addressed also to audiences in the external environment. That after all is where support for the country and its legitimacy in the external operational environment comes from. These policies etc. need to inform the foreign policy position and stance of the country. There is hence an inextricable linkage between domestic policy, national security policy and foreign policy. That eventually is the essence of the world view of propaganda and the corrective measures that it is aimed at. And this is why diplomacy is eventually a core component of all that propaganda tries to do and should try to do.

Conclusions

The issues and problems of propaganda and disinformation have emerged as the new forms of challenges for states, as they try to address emerging – and old – problems of national security. National security and threats to it has always been a core concern of states, and it will remain so for as long as states exist. These state concerns are however taking place in radically different operational environments. In particular, these environments have unleashed the challenges of technology and its interaction with information. This has shaped the colour of the information revolution drastically. All this means that although the problem – national security – still exists, states must adopt new tokens – ways of addressing the problems. The operating environment indeed demands this.

The new threats and their operational arena have also changed. The threats are now operating in an arena that knows no territorial boundaries. The new challenge of the information revolution and its attendant digitalization, and the access of state and non-state actors to it means that in their national security strategizing, states must address both the domestic and international dimensions. This has posed challenges for diplomacy and diplomatic practices, which are called upon to adjust their methodologies to meet the reality and dimensions of the emerging challenges. Some states and their diplomacies are unwilling to do so. In doing so, they have restricted their perceptions of the existing threats to a very narrow regional frame. They have failed to realize that in the presence

of the complex interdependence of the international environment, they are and will always be part of all they have met.

But it is not only diplomacy that is challenged to adjust in this age of digitalization. States responses to it must also adjust. While digitalization poses clear and present dangers to national security, the methods of state interaction with it must be viewed i=through the lenses of a rapidly transformed operational environment. The old strategies of dealing with information are now as outdated as the famous dodo. While legal responses are possible, they are greatly limited now. States need to devise new and forward looking ways to interact with the digitalization that has become a permanent member at their national security table. They need to be creative: as creative as Can Themba's short story in *The Will to Die*, in which a wife was required to set a table for the 'present but absent' partaker of the meal…even where clearly he was not physically present.

Digitalization and digital diplomacy in these perspectives is not and should not ultimately be seen as 'the dark side of diplomacy.' It is a new diplomacy that requires adjustments to the practice of diplomacy, and more creative responses and attitudes to its role as one of the elements of national power, in which it is the first responder in threats to state survival. Digital diplomacy is a mental and intellectual enterprise that can be shaped by the creativity of the operational and tactical aspects of the practice of diplomacy. It needs to develop new and creative ways of countering the threats of propaganda and disinformation that are now abroad. Digital diplomacy in essence lays the ground for responses to the subversion of reality that terrorists and others thrive on engineering. Tactically, it may be seen by diehards of traditional forms of diplomacy as an enterprise of dirtying fingers. Operationally, it may also be seen as an enterprise of dirtying the hands that control the fingers. However the challenge if now more than ever a strategic one: whether it is feasible to sit back and claim that the strategic mind will also be dirties by riding shotgun in the service of national security. This was the theme of this paper.

*** *** ***

End Notes

[1]Makumi Mwagiru, 'The Discipline Extended: The Diplomacy of Global Health' in Makumi Mwagiru, *Diplomacy and Its Relations: Essays on African Perspectives on Contemporary Diplomacy* (Nairobi: IDIS, 2012), pp. 165-176.

[2]Corneliu Bjola & James Pamment, 'Introduction: The 'dark side' of digital diplomacy' in Corneliu Bjola& James Pamment (eds.) *Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy* [Oxford: Routledge, 2019], pp. 1-10::1.

[3]Ibid, p. 21.

[4]Bjola & Pamment, Ibid, p.1.

[5] Ibid, p. 2.

[6]Bjola & Pamment, p. 3.

[7] Hedley Bull & Adam Watson (eds.), *The Expansion of International Society* (Oxford: Clarendon Press, 1989).

[8] James Pamment & Corneliu Bjola, 'Conclusion: Rethinking Strategic Communication in the Digital Age' in Bjola & Pamment (eds.) *Countering Online Propaganda and Extremism*, op. cit., pp. 172-179:175.

[9] Herman Wasserman &Dani Madrid-Morales, 'An Exploratory Study of "Fake News" and Media trust in Kenya, Nigeria and South Africa' *African Journalism Studies*, August, 2019.

[10] Daniela Stefanescu & Teodoru Stefan, 'Countering Violent Radicalization: Lessons Learned' Mihai Viteazul National Intelligence Academy, Bucharest, 2018.

[11] Sean S. Castigan & Jake Perry, *Cyberspaces and Global Affairs* [Burlington, VT: Ashgate, 2013], p. 319.

[12] 'Kenya Will use Security Council seat to oppress Somalia-Djibouti' *Hiraan Online*, Thursday, September 19, 2019.

[13] Ibid.

[14] Chad W. Fitzgerald & Aaron F. Brantly, 'Subverting Reality: The Role of Propaganda in 21st Century Intelligence' *International Journal of Intelligence and Counter Intelligence*, Vol. 30, No. 2 (2017), pp. 215-240.

[15] Fitzgerald & Brantly [2017], p. 218.

[16]Fitzgerald & Brantly [2017] p. 235.

[17]Ibid, p. 236.

[18]Ilan Manor & Rhys Crilley, 'The Aesthetics of Violent Extremism and Counter-Violent Communication' in Bjola & Pamment (eds.), *Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy* [Oxford: Routledge, 2019] pp. 121-139.

[19]Bjola & Pamment, 'Introduction…' op. cit., p. 8.
[20]Manor & Crilley, ibid, p. 139.
[21] David Mitrany, A *Working Peace System* (London: Oxford University Press, 1994).
[22] Mary Dudziak, *War Time: An Idea, Its History, Its Consequences* (New York: Oxford, 2012).