Dieser Text wurde zuerst am 12.05.2023 auf www.mintpressnews.com unter der URL ‹https://www.mintpressnews.com/independent-ukraine-kill-list-actually-run-by-kiev-backed-by-washington/284639/› veröffentlicht.

Symbolbild (Bild: Tumisu, Pixabay, CCo)

Von Kiew geführt und von Washington unterstützt:

„Unabhängige“ ukrainische „Kill-Liste“

Ende letzten Jahres wurde mein Name auf eine Schwarze Liste gesetzt, die vom ukrainischen „Center for Countering Disinformation“ [1] online veröffentlicht wurde. Ich gesellte mich zu über neunzig anderen, von denen behauptet wird, sie verbreiteten „mit der russischen Propaganda übereinstimmende Narrative.“

Autor: David Miller

Professor David Miller ist ein nicht ortsansässiger Senior Research Fellow am Centre for Islam and Global Affairs der Zaim University in Istanbul und ehemaliger Professor für politische Soziologie an der Universität von Bristol. Er ist Rundfunksprecher, Autor und investigativer Forscher, Produzent der wöchentlichen Sendung „Palestine Declassified“ auf PressTV und Co-Direktor von „Public Interest Investigations“, deren Projekte spinwatch.org und po-werbase.info sind. Er twittert unter @Tracking_Power.

Dazu gehörten Manuel Pineda und Clare Daly, beides linke Mitglieder des Europäischen Parlaments (MdEP); ebenfalls auf der Liste stehen Personen der Rechten, wie Doug Bandow vom Cato-Institut, der Neokonservative und ehemalige IDF-Offizier Edward Luttwak, eine Reihe rechter MdEPs, der ehemalige CIA-Offizier Ray McGovern, ehemalige Militärs und Geheimdienstler wie Scott Ritter und Douglas McGregor, sowie Akademiker wie John Mearsheimer und Jeffrey Sachs. Zu den Journalisten auf der Liste gehörten Glenn Greenwald, Tucker Carlson und Eva Bartlett, Roger Waters von Pink Floyd und sogar der Schauspieler Steven Seagal.

Was war mein Verbrechen? Es hieß, mein „pro-russisches Narrativ“ sei die Behauptung, dass „der Stellvertreter-Krieg der NATO mit Russland in der Ukraine stattfindet“. Natürlich ist das, was dort geschieht, ein Stellvertreter-Krieg der NATO, wie dieser Artikel nur noch mehr bestätigen wird.

Die Auflistung enthielt einen Link zu einem Artikel, den ich für Mayadeen English geschrieben habe und der den Titel trägt: „Wie Desinformation funktioniert: der globale Krieg westlicher Geheimdienste gegen die Linke“ [2]. Er enthielt einen einzigen, 176 Wörter langen Absatz über die Ukraine mit dem Titel „‚Russische Desinformation‘ oder ukrainische Lügen?“ Darin wurden mehrere Beispiele für ukrainische Fehlinformationen angeführt und die Schlussfolgerung gezogen, dass „jeder, der eine bestimmte Wahrheit erwähnt, dafür verspottet wird, Putins ‚Talking Points‘ nachzuplappern.“ In der Tat wurde ich als „Informations-Terrorist“ denunziert, der sich möglicher-

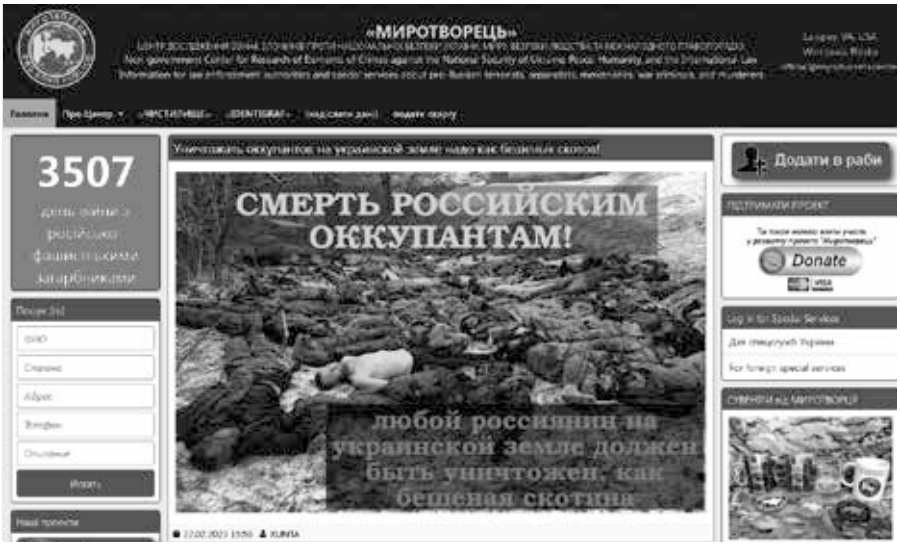
weise „Kriegsverbrechen“ [3] schuldig gemacht habe.

Auf die Schwarze Liste gesetzt zu werden, konzentriert den Geist wunderbar auf die Kräfte, die sich gegen die Möglichkeit von Wahrheit und Gerechtigkeit im krisengeschüttelten Westen stellen. Als ich vor über zehn Jahren zum ersten Mal des Antisemitismus beschuldigt wurde, bestand meine Antwort darin, meine Forschungs- und Schreibtätigkeit über die Organisationen, die mich verleumdet haben, zu intensivieren. Seitdem habe ich einen langen Katalog von Arbeiten über die zionistische Bewegung und die westlichen Propaganda-Aktivitäten verfasst. Natürlich fördern die diffamierenden Angriffe eine Atmosphäre, in der Drohungen in den sozialen Medien ausgesprochen werden können. Aber das Thema Nazismus in der Ukraine wird im Nachhinein als ein entscheidendes Thema unserer Zeit gesehen werden. Und es ist wichtig, sich daran zu erinnern, dass der Grund, warum ich und viele andere von der ukrainischen Regierung und ihren NATO-Unterstützern bedroht werden, der ist, dass wir im Gegenzug drohen, sie als das zu entlarven, was sie sind: Nazi-Kollaborateure.

Die von der NATO unterstützte Kill-Liste

Aber was ist das „Center for Countering Disinformation“? (CCD, Zentrum für die Bekämpfung von Desinformation; Anm. d. Redaktion)

Es ist eine offizielle Regierungseinrichtung, die Ende März 2021 [4] zusammen mit einer ähnlichen Organisation, dem „Center for Strategic Communication“ (and Information Security, CSCIS, Zentrum für strategische Kommunikation und Informationssicherheit; Anm. d. Redaktion) [5], von Präsident Selenskyj selbst gegründet wurde. Aber stehen sie in Verbindung mit anderen Websites mit Schwarzen Listen wie „Myrotvorets“ („Peacemaker“), die weithin als „Kill-Liste“ [6] angesehen werden? Wenn wir die Schichten der Tarnung und Täuschung aufdecken, können wir die Ursprünge der Kill-Liste zurückverfolgen, die immer noch in der Ukraine gehostet wird.



„Wir müssen die Besatzer auf ukrainischem Boden wie wildes Vieh vernichten!" (Screenshot: https://myrotvorets.center/)

Wie sich herausstellte, ist die verdeckte „Kill-Listen“-Website ein Produkt des ukrainischen Regimes, das (unter anderem) von der CIA finanziert und von der NATO betrieben wird.

Außergewöhnlich ist, dass sowohl viele amerikanische Bürger auf der Liste stehen – darunter ehemalige Militärs und Geheimdienstmitarbeiter – als auch eine beträchtliche Anzahl von Bürgern aus NATO-Mitgliedstaaten. Das vielleicht bemerkenswerteste Element ist, dass die NATO die Website (und eine Reihe angeschlossener Websites) auf ihren Servern in Brüssel untergebracht hat. Zur gleichen Zeit, in der die NATO-Denkfabrik „Atlantic Council“ damit prahlt, dass Henry Kissinger in ihrem Vorstand sitzt [7], beherbergt die NATO auch eine Website mit einer Kill-Liste, auf der Kissinger erscheint.

Sie glauben mir nicht? Lassen Sie uns einen Blick darauf werfen.

Beginnen wir mit der Website der Kill-Liste selbst, „Myrotvorets“. Heute befindet sie sich unter Myrotvorets.center, aber ursprünglich war sie unter psb4ukr.org zu finden. Diese Domain wurde erstmals am 14. August 2014 [8] registriert, etwa sechs Monate nach dem von den USA unterstützten Maidan-Putsch, der die demokratisch gewählte Regierung von Viktor Janukowitsch stürzte. Später wurden weitere ähnliche Domainnamen für die Gruppe registriert, darunter die folgenden (Datum der ersten Registrierung in Klammern):

- Psb-news.org [9] (3. April 2015)
- Psb4ukr.ninja [10] (19. April 2015)
- Psb4ukr.net [11] (7. May 2015)
- Psbr4ukr.xyz [12] (8. November 2015)
- Report2psb.online [13] (19. August 2017)

Diese wurden entweder als Spiegelseiten, als Zusammenfassung von Nachrichten der Website oder, im Falle der letzten, als Formular für die Meldung von Verdächtigen genutzt [14]. Der Domänenname Myrotvorets.center wurde erstmals am 7. November 2015 registriert und die Seite war im Februar 2016 online.

Drei Personen werden mit diesen Domänen in Verbindung gebracht, und sie liefern wertvolle Hinweise darauf, wer und was an der Webseite mit der Kill-Liste beteiligt war. Sie sind folgende:

Victor/Viktor Garbar ist ein langjähriger Maidan-Aktivist und Koordinator des „Maidan Monitoring Information Center“ [15]. Er war der erstea Registrant eines Myrotvorets-Domainnamens im August 2014 – psb4ukr.org. Zuvor besaß er bereits seit 2001 die Domain von „Maidan Monitoring“ – maidanua.org [16] (jetzt unter maidan.org.ua). Die Gruppe existierte bereits vor der so genannten „Orangenen Revolution“ im Jahr 2004. Sie wurde natürlich vom „National Endowment for Democracy“ [17],

Publiziert auf Free21 am 21.11.2023, 6:00 Uhr

der als „Handlanger der CIA“ [18] bekannten Stiftung, und dem „International Renaissance Fund“, dem ukrainischen Zweig [19] der von George Soros geführten „Open Society Foundation“, finanziert.

(George Soros hat die Kontrolle über die Open Society-Stiftung mittlerweile seinem Sohn übergeben, Alexander Soros; Anm. d. Redaktion)

Vladimir/Volodymyr Kolesnikov ist ein Webmaster und Entwickler. Er hat nie öffentlich zu erkennen gegeben, dass er mit „Myrotvorets“ in Verbindung steht. Unter den Links, die auf die Kill-Liste verweisen, befindet sich auch eine Domain, die ihm gehört (free-sevastopol.com [20]) und die jetzt auf Myrotvorets.center weiterleitet. Er ließ auch psb-news.org [21] registrieren, das sich den „Myrotvorets“-Nachrichten widmet.

Oksana/Oxana Tinko war die Erste, die die Domain Myrotvorets.center [22] registrierte. Sie registrierte auch mehrere andere [23], die mit dem Kill-Listen-Projekt zusammenhängen, wie z. B. Psb4ukr.ninja [24], Psb4ukr.net und Psbr4ukr.xyz.

Operation Schmetterling – Der Prototyp einer Kill-Liste

Tinko hat auch eine Reihe von Domains registriert, die Komponenten des „Myrotvorets“-Projekts zu sein scheinen sowie eine, die anscheinend ein Prototyp war. Besonders deutlich wird die Absicht, die Website zur Tötung von Verrätern oder „Terroristen“ zu nutzen. Die Domain Metelyk.org wurde erstmals am 21. Juli 2014 [25] beansprucht – drei Wochen vor der ersten Myrotvorets-Domain. „Metelyk“ ist das ukrainische Wort für Schmetterling. Die Website mit dem Titel „Operation Butterfly“ war Ende August 2014 online, die ersten Bestände im Internet-Archiv stammen vom 27. desselben Monats.

In den FAQs der Website wird klargestellt, dass die Forderung nach „Separatismus oder Änderungen des Verfassungssystems“ als Straftat angesehen wird [26]. Auf der Website wird auf die Notwendigkeit hingewiesen, „geeignete Maßnahmen zu ergreifen, wenn das Gericht, die Polizei, der SBU (Inlandsgeheimdienst der Ukraine; Anm. d. Redaktion) oder die Staatsanwaltschaft versuchen, Terroristen und ihre Komplizen aus den Fängen des Gesetzes zu befreien“. In den FAQ wird noch deutlicher, was mit „geeigneten Maßnahmen“ gemeint ist.

F: Letzte Frage: Warum „Schmetterling“?

A: Das Logo der Website zeigt einen Schmetterling, der als „Totenkopfschwärmer“ bekannt ist. Im Lateinischen hat er den Namen Acherontia atropos, wobei das erste Wort vom Namen des Flusses im Reich der Toten in der antiken griechischen Mythologie stammt. Das zweite ist der Name der Schicksalsgöttin, die den Faden des menschlichen Lebens durchschneidet. Diese Symbolik soll die Feinde der Ukraine daran erinnern, dass ihr Schicksal derzeit an einem sehr dünnen Faden hängt, und wir werden alles tun, um diesen Faden zu zerreißen.

Ende 2014 war eine weitere verbundene Website – Operativ.info – in Betrieb, die zu Informationen über Saboteure und Terroristen aufrief und drohte, dass man, falls Desinformation entdeckt würde, „diese Aktionen als Unterstützung für Terroristen betrachten und Maßnahmen gegen Desinformanten ergreifen würde“ [27]. Aufschlussreicherweise wurde die Website Operativ.info zu diesem Zeitpunkt als Projekt von „InformNapalm“ bezeichnet [28].

„Myrotvorets“ listet Tausende von „Saboteuren“, „Separatisten“, „Terroristen“ und „Verrätern“ auf. Manchmal wurden ihre Fotos nach ihrer Ermordung durchgestrichen und mit dem Vermerk „liquidiert“ versehen.

Dies geschah zum Beispiel nach der Ermordung von Daria Dugina in Moskau im August 2022 [29]. Heute enthält die „Myrotvorets“-Website Links zu zwei anderen Domains, die integraler Bestandteil der Operation zu sein scheinen. Die eine – ordilo.org [30] – trägt den Titel „SPEICHERUNG VON INFORMATIONEN ÜBER VERBRECHEN GEGEN DIE UKRAINE“. Die andere – identigraf.center – ermöglicht es verschiedenen Benutzerkategorien, Bilder von Personen für Gesichtserkennungs-Scans einzusenden. Tinko hat beide Domänen registriert [31].

(Screenshot: https://medium.com/@deborahlarmstrong/a-life-worth-one-bullet-6efa4643836b)

Quellen:

[1] Internetarchiv, Center for Countering Disinformation (Ukrainische Regierung) „Спікери, які просувають співзвучні російській пропаганді наративи" in 2022: <*https://web.archive.org/web/20221004031714/https://cpd.gov.ua/reports/spikery-yaki-prosuvayut-spivzvuchni-rosijskij-propagandi-naratyvy* />

[2] Al Mayadeen Nachrichtensender, David Miller „How Disinformation Works: Western Intelligence Agencies' Global War on the Left", am 20.7.2022: <*https://english.almayadeen.net/articles/analysis/how-disinformation-works:western-intelligence-agencies-global-war-on-the-left*>

[3] Newsweek, Nick Reynolds „Meet the Democrat Siding With Putin on the Ukraine War", am 24.8.2022: <*https://www.newsweek.com/meet-democrat-siding-putin-ukraine-war-1736517*>

[4] Center for Countering Disinformation (Ukrainische Regierung), Ankündigung „Відбувся другий Національний кластер з інформаційної стійкості", am 21.9.2023: <*https://cpd.gov.ua/*>

[5] SPRAVDI Zentrum für strategische Kommunikation (Ukraine) „about the center": <*https://spravdi.gov.ua/en/about-us/?__cf_chl_tk=q8X5Bi4KALpR.5u47zeemm_oK3J4NicpYA-8j0uCjja4-1683040462-0-gaNycGzNDXs*>

[6] Morningstar Zeitung, Steve Sweeney „Ukraine publishes list of 'undesirables' accused of supporting the Russian invasion", am 23.5.2022: <*https://morningstaronline.co.uk/article/w/ukraine-publishes-list-of-undesirables-accused-of-supporting-the-russian-invasion*>

[7] Atlantic Council Denkfabrik „Board of Directors": <*https://www.atlanticcouncil.org/about/board-of-directors/*>

[8] Whoxy Domain Suchmaschine „Domain: PSB4UKR.ORG", am 14.8.2014: <*https://www.whoxy.com/psb4ukr.org*>

[9] Whoxy Domain Suchmaschine „Domain: PSB-NEWS.ORG", am 3.4.2015: <*https://www.whoxy.com/psb-news.org*>

[10] Whoxy Domain Suchmaschine „Domain: psb4ukr.ninja", am 19.4.2015: <*https://www.whoxy.com/psb4ukr.ninja*>

[11] Whoxy Domain Suchmaschine „Domain: PSB4UKR.NET", am 27.7.2016: <*https://www.whoxy.com/psb4ukr.net*>

[12] Whoxy Domain Suchmaschine „Domain: psb4ukr.xyz", am 8.11.2015: <*https://www.whoxy.com/psb4ukr.xyz*>

[13] Whoxy Domain Suchmaschine „Domain: report2psb.online", am 19.8.2017:<*https://www.whoxy.com/report2psb.online*>

[14] Internetarchiv, Mirotworez Zentrum „Friedensstifter" (Ukraine): <*https://web.archive.org/web/20180831115739/https://report2psb.online/*>

[15] Linkedin, Viktor Garbar Profil: <*https://www.linkedin.com/in/viktorgarbar/?originalSubdomain=ua*>

[16] Whoxy Domain Suchmaschine „MAIDANUA.ORG", am 21.2.2001: <*https://www.whoxy.com/maidanua.org*>

[17] Maidan Monitoring Information Center Organisation Website: <*https://maidan.org.ua/aboutmaidan/mmic/*>

[18] YouTube, EVILisEVILdoes „The CIA and the National Endowment for Democracy YouTube ", Min. 1:31, am 9.10.2011: <*https://youtu.be/AsdMwi1XQEo?t=91*>

[19] Open Society Foundations Stiftung „The Open Society Foundations in Ukraine", am 18.5.2022: <*https://www.opensocietyfoundations.org/newsroom/the-open-society-foundations-in-ukraine*>

[20] Whoxy Domain Suchmaschine „Domain: FREE-SEVASTOPOL.COM", am 18.9.2010: <*https://www.whoxy.com/free-sevastopol.com*>

Die NATO-Verbindung

Kolesnikov und Tinko waren aufeinanderfolgende Registranten auf Natocdn.work [32] (ab 11. März 2015). Tinko registrierte eine Folgedomain Natocdn.net [33] (28. Januar 2019). Diese obskur klingenden Webadressen wurden verwendet, um die für die „Myrotvorets"-Seite benötigten Dateien zu hosten, wie eine Untersuchung des „Seitenquelltextes" (in Chrome mit der rechten Maustaste anklicken und „Seitenquelltext anzeigen" [34] wählen) auf der Website zeigt, auch in den im Internet-Archiv [35] gespeicherten Versionen.

Der erste Domänenname (.work) wurde zuvor sowohl für die ursprüngliche als auch für die nachfolgende „Myrotvorets"-Website verwendet. So findet er sich im Quellcode von psb4ukr.org am 15. Dezember 2015 [36] – kurz vor dem Start der Website myrotvorets.center – und ist im Quellcode der letztgenannten enthalten, als sie am 25. Februar 2016 erstmals im Internetarchiv erfasst wurde [37]. Das Archiv zeigt auch, dass die letztgenannte Domain später über Natocdn.net gehostet wurde [38].

Die Buchstaben CDN verweisen möglicherweise auf ein Content Delivery Network – ein Gerät zur Beschleunigung der Bereitstellung von Websites – wenn diese von einem ansonsten entfernten Standort aus gesucht werden, wie z. B. die in Kalifornien ansässigen Namensserver, die auch von der Website verwendet werden. Tatsächlich wird die Domäne Natocdn.net bei niemand anderem als der offiziellen Website NATO.int [39] gehostet, die ihren Sitz in Brüssel hat.

Bereits am 17. April 2015 hatten mehrere Interessierte die ursprüngliche Webadresse (psb4ukr.org) ohne die zwischengeschaltete „CDN"-Domain direkt zu nato.int zurückverfolgt, was darauf hindeutet, dass „Myrotvorets" fast von Anfang an dort gehostet wurde [40]. Andere IP-Historien zeigen, dass die oben erwähnte „Operation Butterfly"-Domain ebenfalls auf psb4ukr.nato.int gehostet wurde, ebenso wie zwei weitere Websites [41]:

- zoperativ.info [42], die, wie wir oben festgestellt haben, Teil der Operation „Myrotvorets" war;
- informnapalm.org [43]

Letztere wurde als „anti-russische Propagandaseite" bezeichnet [44]. Das ist zwar sicherlich richtig, doch unterschätzt diese Bezeichnung die Bedeutung dieser Domain für diese Geschichte erheblich, wie wir sehen werden.

Etwa einen Tag nach dieser Enthüllung im April 2015 registrierte Oxana Tinko eine neue Website für das Projekt: psb4ukr.ninja [45]. Vielleicht törichterweise, vielleicht in dem Versuch, sich an die Enthüllung anzulehnen, gab sie ihren Standort als Estland und ihr Unternehmen als NATO CCD COE an – das „NATO Cooperative Cyber Defense Center of Excellence". Um die Authentizität zu erhöhen, gab sie die richtige Adresse und Telefonnummer an.

Das NATO-Center gab rasch eine Erklärung ab, in der jegliche Verbindung geleugnet wurde [46]:

„Tatsächlich hat das Exzellenzzentrum keinerlei Verbindung zu der erwähnten Website ... Oxana Tinko ... hat keinerlei Verbindung zum NATO Cooperative Cyber Defence Centre of Excellence ... [Sie] scheint die öffentlichen Informationen des Zentrums gekapert zu haben, und wir unternehmen Schritte, um die falschen Informationen zu entfernen."

Es ist jedoch auch bemerkenswert, dass eine PowerPoint-Präsentation des ukrainischen Verteidigungsministeriums aus dem Jahr 2015, die im April desselben Jahres durchgesickert ist, das NATO-Cyberzentrum als eine von sieben westlichen Gruppen nennt, mit denen es eine „Zusammenarbeit" gab [47].

Dennoch blieb der Link zu den NATO-Servern im Quellcode der „Myrotvorets"-Websites erhalten. Erst als die NATO-Verbindung Ende August 2022 wieder zum Thema wurde, wurde etwas dagegen unternommen. Dies geschah, nachdem Henry Kissinger der Seite im Mai hinzugefügt worden war. Am 24. August berichtete die unabhängige Journalistin Eva Bartlett (die sowohl auf der „Myrotvorets"-Liste als auch auf der Liste des „Center for Countering Disinformation" genannt wurde), dass der Quellcode der Myrotvorets-Seite Links zu Ressourcen auf psb4ukr.natocdn.net enthielt [48]. Später, am 14. Oktober, machte sie auf die Tatsache aufmerksam, dass Elon Musk kurzzeitig auf der

„Das Offiziershandbuch der russischen Streitkräfte mit dem "DSP"-Stempel, aufgegeben an den Standorten der "SVO" – eine Diagnose für die russische Armee.
Während der erfolgreichen Offensivoperationen der ukrainischen Streitkräfte im Gebiet ROBOTINO in der Region Saporoschje und der Einnahme russischer Stellungen wurde das Handbuch eines Offiziers der russischen Armee mit dem Stempel "For Official Use" gefunden. Eine Scan-Kopie dieses Handbuchs kann hier eingesehen werden (PDF)"
(Screenshot: https://informnapalm.org/52801-spravochnik-oficera-vs-rf-s-grifom-dsp/)

Seite aufgeführt war, nachdem er damit gedroht hatte, sein Starlink-System nicht mehr kostenlos an das ukrainische Militär zu liefern. Musk antwortete daraufhin: „Ist diese Liste echt?“ Innerhalb von acht Tagen waren die Links zu natocdn.net aus dem Quellcode verschwunden.

Mehr als einhundert Links zu natocdn.net waren am 21. Oktober 2022 um 22:35 Uhr [49] noch vorhanden, aber am nächsten Morgen um 09:14 Uhr [50] waren sie alle verschwunden. Selbst nachdem der belastende Text entfernt wurde, zeigen IP-Tracking-Seiten jedoch immer noch [51], dass die Domäne natocdn.net zum Zeitpunkt der Erstellung dieses Berichts (Archivversion [52]) auf Servern im NATO-Hauptquartier in Brüssel liegt. Tatsächlich werden viele der Bilddateien, die für die Website verwendet wurden, immer noch unter dieser URL gehostet, einschließlich der blutigen Collage mit angeblich toten russischen Soldaten [53] auf der Titelseite (Archivversion [54]).

Aber was ist mit Informnapalm.org – der anderen Website, die anscheinend auf nato.int gehostet wurde? Die Beweise legen nahe, dass „Myrotvorets“ ein Projekt von „InformNapalm“ ist.

InformNapalm als „Sonderprojekt“ des ukrainischen Verteidigungsministeriums

„InformNapalm“ gibt sich als ehrenamtlich geführter Nachrichtendienst aus. Doch das ist eine Täuschung. In einer 2015 durchgesickerten PowerPoint-Präsentation des ukrainischen Verteidigungsministeriums wird „InformNapalm“ als „spezielles Projekt“ des Ministeriums bezeichnet [55] – zusammen mit einer Reihe anderer, die ebenfalls einer weiteren Untersuchung bedürfen.

Quellen:

[21] Whoxy Domain Suchmaschine „Domain: PSB-NEWS.ORG", am 3.4.2015: *<https://www.whoxy.com/psb-news.org>*

[22] Whoxy Domain Suchmaschine „Domain: MYROTVORETS.CENTER", am 6.11.2015: *<https://www.whoxy.com/myrotvorets.center>*

[23] Whoxy Domain Suchmaschine, Oksana Tinko, Anmeldung diverser Domains, zwischen 2014 und 2019: *<https://www.whoxy.com/name/13691208>*

[24] Whoxy Domain Suchmaschine „Whois Lookup of psb4ukr.ninja", Datum unbekannt: *<https://www.whoxy.com/psb4ukr.ninja>*

[25] Whoxy Domain Suchmaschine „METELYK.ORG", am 21.7.2014: *<https://www.whoxy.com/metelyk.org>*

[26] Internetarchiv, Operation Butterfly (Metelyk.org) Todesliste, FAQ: *<https://web.archive.org/web/20141216203948/http://metelyk.org/чапи-faq/>*

[27] Internetarchiv, Operativ.info „Сообщить о предателе или диверсанте – Сообщить о событии", in 2014: *<https://web.archive.org/web/20141116034151/https://operativ.info/>*

[28] Internetarchiv, Operativ.info „Сообщить о предателе или диверсанте – Сообщить о событии", in 2014: *<https://web.archive.org/web/20141116034151/https://operativ.info/>*

[29] Medium Publishing-Plattform, Deborah L. Armstrong „A Life Worth One Bullet – "Info-Terrorist" and "Russian Separatist," 13-year old Faina Savenkova", am 18.10.2022: *<https://medium.com/@deborahlarmstrong/a-life-worth-one-bullet-6efa4643836b>*

[30] Internetarchiv, Suchbegriff „ordilo.org", zwischen 7.8.2016 und 25.9.2023: *<https://web.archive.org/web/20230000000000*/ordilo.org>*

[31] Whoxy Domain Suchmaschine, oxana.tinko@gmail.com, Anmeldung diverser Domains (15) zwischen 2014 und 2019: *<https://www.whoxy.com/email/33904452>*

[32] Whoxy Domain Suchmaschine „Domain: NATOCDN.WORK", am 9.6.2021: *<https://www.whoxy.com/natocdn.work>*

[33] Whoxy Domain Suchmaschine „Domain: NATOCDN.NET", am 26.1.2019: *<https://www.whoxy.com/natocdn.net>*

[34] Snappy easy peasy tutorials „View source code of a webpage in Chrome | Chrome Tutorial #13", am 27.10.2017: *<https://www.youtube.com/watch?v=_bj8G597Qds&ab_channel=Snappy–easypeasytutorials>*

[35] Internetarchiv, Suchbegriff „myrotvorets.center", zwischen 25.2.2016 und 26.9.2023: *<https://web.archive.org/web/20230000000000*/myrotvorets.center>*

[36] Internetarchiv „МИРОТВОРЕЦ" DAS ZENTRUM FÜR DIE ERFORSCHUNG DER ZEICHEN VON VERBRECHEN GEGEN DIE NATIONALE SICHERHEIT DER UKRAINE, DEN FRIEDEN, DIE SICHERHEIT DER MENSCHHEIT UND DAS INTERNATIONALE RECHT UND DIE ORDNUNG", am 15.12.2015: *<https://web.archive.org/web/20151215084644/https://psb4ukr.org/>*

[37] Internetarchiv, „МИРОТВОРЕЦ", am 25.2.2016: *<https://web.archive.org/web/20160225060820/https://myrotvorets.center/>*

[38] Internetarchiv „МИРОТВОРЕЦ", am 25.2.2016: *<https://web.archive.org/web/20160225060820/https://myrotvorets.center/>*

[39] MYIP.MS IP-Adressen-Suchmaschine „Whois Web Hosting Information for website – natocdn.net – ", am 19.6.2014: *<https://whatmyip.co/info/whois/152.152.31.120/k/147021221/website/natocdn.net>*

[40] Indian Defence Forum, Cadian „Ukrainian WEB resorces hosted by NATO ", am 17.4.2015: *<https://defenceforumindia.com/threads/ukrainian-web-resorces-hosted-by-nato.67645/>*

Quellen:

[41] Indian Defence Forum, Cadian „Ukrainian WEB resorces hosted by NATO ", am 17.4.2015: <*https://defenceforumindia.com/threads/ukrainian-web-resorces-hosted-by-nato.67645/*>

[42] Internetarchiv, Suchbegriff „operativ.info", zwischen 12.1.2012 und 24.9.2023: <*https://web.archive.org/web/20230000000000*/operativ.info*>

[43] Inform Napalm Website: <*https://informnapalm.org/*>

[44] Indian Defence Forum, Cadian „Ukrainian WEB resorces hosted by NATO ", am 17.4.2015: <*https://defenceforumindia.com/threads/ukrainian-web-resorces-hosted-by-nato.67645/*>

[45] Whoxy Domain Suchmaschine „Whois Lookup of psb4ukr.ninja": <*https://www.whoxy.com/psb4ukr.ninja*>

[46] CCDCOECenter for Cyber Defence Centre of Excellence „Statement Regarding Connection to Foreign Websites": <*https://ccdcoe.org/news/2015/statement-regarding-connection-to-foreign-websites/*>

[47] drakulablogdotcom3, Präsentation „FREE RUSSIA – Plan of information ad psychological operation", im April 2014: <*https://drakulablog-dotcom3.files.wordpress.com/2015/04/free-russia.ppsx*>

[48] Telegram, Eva Karene Bartlett „Reality Theories", am 24.8.2022: <*https://t.me/s/Reality_Theories?q=nato.int*>

[49] Internetarchiv „МИРОТВОРЕЦЬ", am 21.10.2022: <*https://web.archive.org/web/20221021223514/https://myrotvorets.center/*>

[50] Internetarchiv „МИРОТВОРЕЦЬ", am 22.10.2022: <*https://web.archive.org/web/20221022091405/https://myrotvorets.center/*>

[51] MYIP.MS IP-Adressen-Suchmaschine „Whois Web Hosting Information for website – natocdn.ne – ", am 19.6.2014 : <*https://whatmyip.co/info/whois/152.152.31.120/k/2768320800/website/natocdn.net*>

[52] archive.today, MYIP.MS IP-Adressen-Suchmaschine „Whois Web Hosting Information for website – natocdn.net -", am 1.5.2023: <*https://archive.ph/FlrxL*>

[53] [psb4ukr.org Website (Ukraine) „СМЕРТЬ РОСІЙСЬКО-ФАШИСТСЬКИМ ЗАГАРБНИКАМ ТА ОКУПАНТАМ!„МИРОТВОРЕЦЬ", Datum unbekannt: <*https://psb4ukr.natocdn.net/2022/05/sm-2048x1365.jpg*>

[54] archive.today, Bildschirmfoto von psb4ukr.natocdn.net „СМЕРТЬ РОСІЙСЬКО-ФАШИСТСЬКИМ ЗАГАРБНИКАМ ТА ОКУПАНТАМ!„МИРОТВОРЕЦЬ", am 6.5.2023: <*https://archive.ph/TNVJ1*>

[55] drakulablogdotcom3, Präsentation „FREE RUSSIA – Plan of information ad psychological operation", im April 2014: <*https://drakulablog-dotcom3.files.wordpress.com/2015/04/free-russia.ppsx*>

[56] Whoxy Domain Suchmaschine „Domain: INFORMNAPALM.ORG (8 similar domains)", am 29.3.2014: <*https://www.whoxy.com/informnapalm.org*>

[57] Inform Napalm, Red. „Help InformNapalm volunteer beat cancer!", am 8.6.2018: <*https://informnapalm.org/en/help-informnapalm/*>

[58] Linkedin „ Volodymyr Kolesnykov "Senior Software Engineer (Services & Solutions) at Automattic WordPress VIP "": <*https://www.linkedin.com/in/volodymyr-kolesnykov/?originalSubdomain=ua*>

[59] Internetarchiv, Cyber-Berkut (rss. Hackergruppe) „BERICHT – Die folgenden Ressourcen wurden bei der Untersuchung der Netzinfrastruktur von A. Geraschtschenko ermittelt: (...)", Datum unbekannt: <*https://web.archive.org/web/20161010105352/http://cyber-berkut.org/docs/Texomчem.rtf*>

Bestätigende Informationen kommen in Form der Identität der Person – der bereits erwähnte Vladimir Kolesnikov. Dieser hat den Domänennamen informnapalm.org am 29. März 2014 [56] registriert, sechs Monate bevor die erste der Kill-Listen-Domänen registriert wurde. Kolesnikov ist der Webmaster von „InformNapalm" [57]. Auf seiner Linkedin-Seite wird seine Beteiligung an „InformNapalm" so beschrieben, dass er im Februar 2014 als „Übersetzer" begann, im März 2014 zum System-Administrator aufstieg und im April 2014 zum DevOps-Ingenieur [58] (vereinfacht „IT-Fachmann"; Anm. d. Redaktion). Hilfreich ist, dass Vladimir eine weitere „freiwillige" Rolle vom Februar 2014 beim Verteidigungsministerium der Ukraine aufführt. Diese Rolle beinhaltete: „Teilnahme an Informations-Operationen im Interesse der Anti-Terror-Operation in den Gebieten Donezk und Luhansk und Unterstützung bei der Bekämpfung von Informations-Angriffen der Russischen Föderation." „Myrotvorets" ist also ein Projekt von „InformNaplam", das seinerseits ein „Sonderprojekt" des Verteidigungsministeriums ist.

Zu den weiteren Verbindungen zwischen den beiden Projekten gehört, dass Oksana Tinko bei der Registrierung der Domain Myrotverots.center ihre informnapalm.org-E-Mail-Adresse verwendet hat. Auf ihrer Facebook-Seite gibt sie an, seit März 2014 bei „InformNapalm" zu arbeiten. Dies stimmt mit den von der russischen Hackergruppe „Cyber-Berkut" veröffentlichten Daten überein, aus denen hervorgeht, dass Tinko am 29. März 2014 Administratorin der Websites Operativ.info und informnapalm.org geworden war [59].

Tinko zeigt in ihren sozialen Medien gerne Nazi- und Bandera-Symbole. Auf ihrer Github-Seite [60] ist ein Hakenkreuz zu sehen – und ihr Facebook-Profil zeigt einen Hintergrund mit den roten und schwarzen Farben Banderas und einem Davidstern zusammen mit einem als orthodoxer Jude verkleideten Reptil [61].

Der Journalist George Eliason, der einen Großteil der Geschichte von „InformNapalm" ausgegraben hat, berichtet, dass es sich bei den beteiligten Personen „größtenteils um Pravy Sektor" (Rechter Sektor) [62] handelt, also um rechtsextreme Anhänger von Stepan Bandera. Der Pravy Sektor verwendet die roten und schwarzen Farben von Bandera in seiner Flagge [63], genau wie Tinko auf ihrem Facebook-Profil. Ende 2019 zeigte „Myrotvorets" anlässlich des Geburtstages des Nazi-Kollaborateurs stolz ein Porträt von Bandera auf seiner Homepage.

In den Anfangstagen des „Myrotvorets"-Projekts war das „InformNapalm"-Logo gut sichtbar angebracht. Am 13. Mai 2016 war es noch da [64], aber im August desselben Jahres war es verschwunden. Der Grund dafür könnte die Veröffentlichung der Liste mit den Namen von Tausenden von Journalisten gewesen sein, die erhebliche Reaktionen hervorrief [65] und zu einer Erklärung führte, dass „das Zentrum ‚Peacemaker' angesichts der Reaktionen ... die schwierige Entscheidung getroffen hat, die Seite zu schließen." Die Seite wurde jedoch nicht geschlossen. Im Jahr 2017 prahlte „Myrotvorets" weiterhin mit seinen Verbindungen zu „InformNapalm" [66] und erklärte:

„Freiwillige Mitarbeiter der ukrainischen Cyber-Allianz (UCA), der Nachrichtendienst InformNapalm und das Peacemaker Center veröffentlichen ihre Recherchen auf der Grundlage von Informationen, die in der Post von Terroristen und russischen Behörden enthalten sind."

Wie dieser Abschnitt zeigt, arbeiteten alle drei Organisationen eng zusammen.

Es hat den Anschein, dass „InformNapalm" die übergeordnete oder koordinierende Einrichtung für ein sich entwickelndes Team von pro-ukrainischen Hackern, Forschern, Journalisten und Anhängern der extremen Rechten ist. „InformNapalm" behauptet, dass „wir [uns] hauptsächlich auf offene Quellen [stützen] und verschiedene OSINT-Methoden (= Open Source Intelligence; Anm. d. Redaktion) der Informationsbeschaffung [einsetzen]. Wir erhalten auch einige Informationen von Insidern (HUMINT = Human Intelligence; Anm. d. Redaktion) und Hacktivisten". Sie behauptet außerdem: „InformNapalm beteiligt sich nicht an Computer-Hacking-Aktivitäten und unterstützt diese auch nicht."

Dies ist ein Eingeständnis des Erhalts von nachrichtendienstlichen Informationen („HUMINT") von ukrainischen und

Porträt Banderas am Rathaus Kiew während des Euromaidan am 14. Januar 2014. (Foto: spoilt.exile, Wikimedia Commons,CC-BY-SA.-2.0)

vielleicht auch anderen Geheimdiensten. Die Leugnung der Beteiligung am Hacking oder der Ermutigung dazu wird durch ihre eigenen Erklärungen untergraben, wie in dieser von einem der Hacker [67]:

„Zuerst hatten wir eine eigene Gruppe namens RUH8... Unsere Zusammenarbeit mit anderen Hackergruppen kam dank InformNapalm zustande... wo wir alle Informationen zur Bearbeitung und Veröffentlichung einreichten."

RUH8 ist eine Abkürzung für „Russia Hate". „InformNapalm" behauptete im Jahr 2020, dass es sich „um ein rein ehrenamtliches Projekt handelt, das von keiner Regierung oder einem Geber finanziell unterstützt wird" [68]. Dies ist natürlich eine Lüge.

Prometheus

Es ist öffentlich bekannt, dass „InformNapalm" vom CIA-Proxy „National Endowment for Democracy" finanziert wurde [69]. So berichtet das NED in seiner inzwischen gelöschten Liste der Finanzierungen für die Ukraine im Jahr 2016 [70] zum Beispiel, dass 100.000 US-Dollar für ein Projekt von „Prometheus" [71] bereitgestellt wurden. Es würde „Open-Source-Untersuchungen durchführen, die externe russische Militäraktionen überwachen und aufzeigen, sowie sie auf seiner beliebten und vertrauenswürdigen Website https://informnapalm.org veröffentlichen" [72]. Die „Prometheus"-Domain Prometheus.ngo wurde ebenfalls von Volodymyr Kolesnikov am 11. März 2016 registriert [73].

„Prometheus" wirbt für zwei „Informationspartner" in seinem Betrieb, „InformNapalm" und „The Ukraine Media Crisis Center". „InformNapalm", das Anfang 2014 gegründet wurde, wurde offensichtlich erst ein Projekt von „Prometheus", nachdem letzteres 2016 gegründet wurde.

Das „Ukraine Crisis Media Center" ist natürlich ein weiteres vom Westen finanziertes Projekt [74]. Auf seiner Website [75] gibt es sogar eine lange Liste westlicher staatlicher Finanzierungen zu (u.a. USAID, Botschaften der USA, der Niederlande, der Schweiz, Finnlands, Norwegens, Schwedens und Deutschlands). Ebenso wie militärische/geheimdienstliche Geldgeber wie das NED, die NATO, das in Großbritannien ansässige „Institute for Statecraft" (ein militärischer Geheimdienst), Regimewechsel-Enthusiasten des Soros-Stiftungsnetzwerks und die

Quellen:

[60] GitHub Onlinedienst, Oksana Tinko: <*https://github.com/oxanatinko*>

[61] Facebook, Oksana Tinko: <*https://www.facebook.com/oxanatinko/*>

[62] Substack Onlineplattform, George Eliason „Meet Alice! The DNC Hacker That Clears Julian Assange", am 22.3.2022: <*https://georgeeliason.substack.com/p/meet-alice-the-dnc-hacker-that-clears*>

[63] Prawyj Sektor politische Partei/Organisation „The main accents": <*https://pravyysektor.info/main-accents*>

[64] Internetarchiv, „МИРОТВОРЕЦЬ" „Об оперативной обстановке на информационном фронте 13.05.2016": <*https://web.archive.org/web/20160513184218/https://myrotvorets.center/*>

[65] Internetarchiv, „МИРОТВОРЕЦЬ" „Об оперативной обстановке на информационном фронте 13.05.2016": <*https://web.archive.org/web/20160513184218/https://myrotvorets.center/*>

[66] Internetarchive, „МИРОТВОРЕЦЬ" „О порядке информирования о деятельности Центра «Миротворец»", am 24.2.2017: <*https://web.archive.org/web/20170228202358/https://myrotvorets.center/*>

[67] Inform Napalm, Red. „Ukrainian hacktivists, cyber warfare and vulnerabilities in the public sector – interview with the speaker of the Ukrainian Cyber Alliance", am 2.9.2021: <*https://informnapalm.org/en/uca-hacktivists-2021/*>

[68] Twitter, InformNapalm „InformNapalm is a purely volunteer endeavor which does not have any financial #support from any government or donor. (...)", am 6.5.2020: <*https://twitter.com/InformNapalm/status/1257985047073828864*>

[69] Mintpress Magazin, Alan Macleod „Documents Reveal US Gov't Spent $22M Promoting Anti-Russia Narrative in Ukraine and Abroad", am 18.2.2022: <*https://www.mintpressnews.com/documents-reveal-us-ned-spent-22m-promoting-anti-russia-narrative-ukraine/279734/*>

[70] Mintpress Magazin, Alan Macleod „Documents Reveal US Gov't Spent $22M Promoting Anti-Russia Narrative in Ukraine and Abroad", am 18.2.2022: <*https://www.mintpressnews.com/documents-reveal-us-ned-spent-22m-promoting-anti-russia-narrative-ukraine/279734/*>

[71] Internetarchiv, NED National Endowment for Democracy „Ukraine 2016", am 1.3.2017: <*https://web.archive.org/web/20170322214324/http://www.ned.org/region/central-and-eastern-europe/ukraine-2016/*>

[72] Inform Naplam Website: <*https://informnapalm.org/*>

[73] Whoxy Domain Suchmaschine „Domain: PROMETHEUS.NGO", am 3.3.2016: <*https://www.whoxy.com/prometheus.ngo*>

[74] Mintpress Magazin, Alan Macleod „Documents Reveal US Gov't Spent $22M Promoting Anti-Russia Narrative in Ukraine and Abroad", am 18.2.2022: <*https://www.mintpressnews.com/documents-reveal-us-ned-spent-22m-promoting-anti-russia-narrative-ukraine/279734/*>

[75] Ukraine Crisis media center „Who we are": https://uacrisis.org/en/pro-nas<*https://uacrisis.org/en/pro-nas*>

[76] Ukraine Crisis media center „Donors": https://uacrisis.org/en/donors <*https://uacrisis.org/en/donors*>

[77] Mintpress Magazin, Alan Macleod „How Bellingcat Launders National Security State Talking Points into the Press" am 9.4.2021: <*https://www.mintpressnews.com/bellingcat-intelligence-agencies-launders-talking-points-media/276603/*>

[78] Inform Napalm „Search Results for: MH17": https://informnapalm.org/en/?s=MH17›

„Open Information Partnership“ [76], ein vom MI6 finanziertes Projekt aus Großbritannien, an dem Bellingcat und andere MI6-Auftragnehmer beteiligt waren/sind.

Eine Lawine westlicher Gelder ist in diese Organisationen geflossen, die sich offenbar alle Mühe gegeben haben, ihre wahren Ursprünge und Verbindungen (auch untereinander) zu verschleiern, ganz zu schweigen von ihren Verbindungen zur extremen Bandera-Rechten.

Zurück zur NATO

„InformNapalm“ rühmt sich in seiner Erfolgsliste der engen Zusammenarbeit mit von der NATO betriebenen Gruppen wie dem „Atlantic Council Digital Forensic Lab“ und dem MI6/CIA-Ableger Bellingcat [77]. Man behauptet, „Personen identifiziert zu haben, die in den Abschuss von Flug MH17 [78] verwickelt sein könnten ... (diese Informationen wurden in den Berichten unserer Kollegen vom Bellingcat-Team verwendet).“ Die Organisation behauptet auch, „eine exklusive Analyse von SurkovLeaks [79] durchgeführt zu haben – dem E-Mail-Dump, der zum Empfangsbüro des [russischen Politikers] Surkov gehört und der von der ukrainischen Cyber-Allianz beschafft wurde (die Echtheit der E-Mails wurde von mehreren seriösen Organisationen bestätigt, darunter dem DFR Lab des Atlantic Council)“. Das DFR Lab und Bellingcat sind keine „seriösen“ Organisationen, sondern gehören zu den Informations-Operationen der NATO gegen Russland.

Diese Prahlerei rückt sowohl das DFR-Labor als auch Bellingcat als Kollaborateure der Nazi-Kill-Liste ins Bild, die ihrerseits auf den von beiden Gruppen entwickelten OSINT-Techniken beruht. Jetzt, da wir wissen, dass die „Freiwilligen“ von „Mirotvorets“, „InformNapalm“ und der „Ukraine Hacker Alliance“ ein Projekt der ukrainischen Regierung mit erheblicher NATO-Unterstützung sind, scheint die Rolle des DFR Labs und von Bellingcat Teil dieser Unterstützung für die Nazi-Kill-Liste zu sein.

Im Westen versuchen diese Nazi-Kollaborateure und Apologeten, eine ganz und gar sanftere Darstellung zu verbreiten. So versuchte sich Eliot Higgins vom „InformNapalm“-„Kollegen“ Bellingcat in einem vermutlich herablassenden Dementi, als er twitterte [80]: „„Myrotvorets ist eine Kill-Liste der ukrainischen Regierung‘ wird schnell zum effektivsten Mittel, um die dümmsten Leute auf dieser Website zu identifizieren.“

Wir finden sogar Aric Toler, ebenfalls von Bellingcat, der „Myrotvorets“ kritisiert und gleichzeitig zu leugnen scheint, dass Bellingcat mit „Myrotvorets“ zusammengearbeitet hat. Als Reaktion darauf verteidigte der Gründer von „InformNapalm“ (und vermutlich auch von „Myrotvorets“), Roman Burko, die Aktivitäten der Kill-Liste als reine Stilfrage.

Die vorliegenden Beweise stützen also die Behauptung, dass die NATO in der Ukraine einen Stellvertreter-Krieg führt. Es gibt eine Verbindung zwischen der Nazi-Kill-Liste und der Schwarzen Liste, auf die ich gesetzt wurde insofern, dass beide Operationen des Regimes in Kiew sind. Eine weitere Verbindung ist der stellvertretende Leiter des vom Regime geschaffenen „Center for Strategic Communication“, Mykola Balaban [81, 82]. Er hat seine Erfahrungen mit der „InformNapalm“/“Mirotvorets“-Operation gesammelt, wie aus einem von den russischen Hackern „Cyber-Berkut“ Ende 2015 veröffentlichten Dokument hervorgeht – in welchem er ab November 2014 als Administrator der Websites operativ.info und informnapalm.org auftaucht [83].

Ein wesentlicher Grund dafür, dass die Nazi-Kill-Liste online bleibt, ist wahrscheinlich, dass sie vom Regime in Kiew, der US-Regierung und der NATO geschützt wird.

Quellen:

[79] Inform Napalm, Red. SurkovLeaks (part 2): hacktivists publish new email dump„", am 11.3.2016: *<https://informnapalm.org/en/surkovleaks-part2/>*

[80] TwitterEliot Higgins, „"Myrotvorets is a Ukrainian government kill list" is rapidly becoming the most effective way to identify the dumbest people in this website.", am 15.10.2022: *<https://twitter.com/EliotHiggins/status/1581290949006659584?s=20&t=yfamW0fsm_vAM9XkGAeYCg>*

[81] Twitter, Mykola Balaban Profil: *<https://twitter.com/MykolaBalaban>*

[82] Linkedin, Mykola Balaban Profil: *<https://www.linkedin.com/in/mykola-balaban-356b4427/?originalSubdomain=ua>*

[83] Internetarchiv, Cyber-Berkut (rss. Hackergruppe) „BERICHT – Die folgenden Ressourcen wurden bei der Untersuchung der Netzinfrastruktur von A. Geraschtschenko ermittelt: (...)", Datum unbekannt: *<https://web.archive.org/web/20161010105352/http://cyber-berkut.org/docs/Texom4em.rtf>*